US012118121B2

(12) **United States Patent**
Brannon et al.

(10) **Patent No.: US 12,118,121 B2**
(45) **Date of Patent: *Oct. 15, 2024**

(54) **DATA SUBJECT ACCESS REQUEST PROCESSING SYSTEMS AND RELATED METHODS**

(71) Applicant: **OneTrust, LLC**, Atlanta, GA (US)

(72) Inventors: **Jonathan Blake Brannon**, Smyrna, GA (US); **Casey Hill**, Atlanta, GA (US)

(73) Assignee: **OneTrust, LLC**, Atlanta, GA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 296 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **17/745,829**

(22) Filed: **May 16, 2022**

(65) **Prior Publication Data**

US 2022/0277103 A1 Sep. 1, 2022

Related U.S. Application Data

(63) Continuation-in-part of application No. 17/475,241, filed on Sep. 14, 2021, now Pat. No. 11,334,682, (Continued)

(51) **Int. Cl.**
G06F 21/60 (2013.01)
G06F 21/62 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/6245*** (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/6245
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,536,866 A 8/1985 Jerome et al.
4,574,350 A 3/1986 Starr
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2875255 12/2013
CA 3056394 3/2021
(Continued)

OTHER PUBLICATIONS

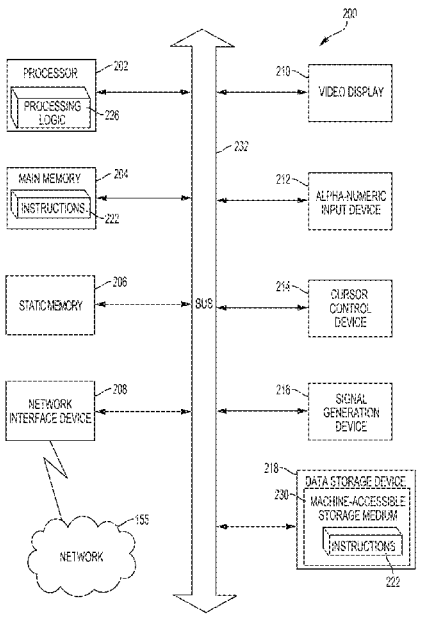
Alkalha et al, "Investigating the Effects of Human Resource Policies on Organizational Performance: An Empirical Study on Commercial Banks Operating in Jordan," European Journal of Economics, Finance and Administrative Science, pp. 1-22 (Year: 2012).
(Continued)

Primary Examiner — Hanh Thi-Minh Bui
(74) *Attorney, Agent, or Firm* — Keller Preece PLLC

(57) **ABSTRACT**

In particular embodiments, computer-implemented data processing, systems, and method configured to: receive a request to initiate a transaction between an entity and a data subject, generate (i) a consent receipt for the transaction comprising at least a unique subject identifier and a unique consent receipt key and (ii) a unique cookie to identify the data subject's transaction initiated by the data subject, store the consent receipt for the transaction and the unique cookie, receive a data subject access request from the data subject, verify an identity of the data subject based at least in part on the unique cookie process the request, process the request by identifying one or more pieces of personal data associated with the data subject, and taking one or more actions based at least in part on the data subject access request.

18 Claims, 71 Drawing Sheets



Related U.S. Application Data

which is a continuation of application No. 17/135,445, filed on Dec. 28, 2020, now Pat. No. 11,120,161, which is a continuation of application No. 16/983,536, filed on Aug. 3, 2020, now Pat. No. 10,878,127, which is a continuation-in-part of application No. 16/881,832, filed on May 22, 2020, now Pat. No. 11,210,420, which is a continuation-in-part of application No. 16/834,812, filed on Mar. 30, 2020, now Pat. No. 10,929,559, which is a continuation of application No. 16/563,741, filed on Sep. 6, 2019, now Pat. No. 10,607,028, which is a continuation-in-part of application No. 16/410,566, filed on May 13, 2019, now Pat. No. 10,452,866, which is a continuation-in-part of application No. 16/055,083, filed on Aug. 4, 2018, now Pat. No. 10,289,870, which is a continuation-in-part of application No. 15/996,208, filed on Jun. 1, 2018, now Pat. No. 10,181,051, which is a continuation-in-part of application No. 15/853,674, filed on Dec. 22, 2017, now Pat. No. 10,019,597, which is a continuation-in-part of application No. 15/619,455, filed on Jun. 10, 2017, now Pat. No. 9,851,966, which is a continuation-in-part of application No. 15/254,901, filed on Sep. 1, 2016, now Pat. No. 9,729,583, said application No. 16/881,832 is a continuation-in-part of application No. 16/552,765, filed on Aug. 27, 2019, now Pat. No. 10,678,945, which is a continuation-in-part of application No. 16/277,568, filed on Feb. 15, 2019, now Pat. No. 10,440,062, which is a continuation-in-part of application No. 16/159,634, filed on Oct. 13, 2018, now Pat. No. 10,282,692, which is a continuation-in-part of application No. 16/055,083, filed on Aug. 4, 2018, now Pat. No. 10,289,870, which is a continuation-in-part of application No. 15/996,208, filed on Jun. 1, 2018, now Pat. No. 10,181,051, which is a continuation-in-part of application No. 15/853,674, filed on Dec. 22, 2017, now Pat. No. 10,019,597, which is a continuation-in-part of application No. 15/619,455, filed on Jun. 10, 2017, now Pat. No. 9,851,966, which is a continuation-in-part of application No. 15/254,901, filed on Sep. 1, 2016, now Pat. No. 9,729,583.

(60) Provisional application No. 62/852,832, filed on May 24, 2019, provisional application No. 62/728,435, filed on Sep. 7, 2018, provisional application No. 62/360,123, filed on Jul. 8, 2016, provisional application No. 62/353,802, filed on Jun. 23, 2016, provisional application No. 62/348,695, filed on Jun. 10, 2016, provisional application No. 62/541,613, filed on Aug. 4, 2017, provisional application No. 62/537,839, filed on Jul. 27, 2017, provisional application No. 62/547,530, filed on Aug. 18, 2017, provisional application No. 62/572,096, filed on Oct. 13, 2017, provisional application No. 62/631,684, filed on Feb. 17, 2018, provisional application No. 62/631,703, filed on Feb. 17, 2018.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,193,162	A	3/1993	Bordsen et al.
5,276,735	A	1/1994	Boebert et al.
5,329,447	A	7/1994	Leedom, Jr.
5,404,299	A	4/1995	Tsurubayashi et al.
5,535,393	A	7/1996	Reeve et al.
5,560,005	A	9/1996	Hoover et al.
5,668,986	A	9/1997	Nilsen et al.
5,710,917	A	1/1998	Musa et al.
5,761,529	A	6/1998	Raji
5,764,906	A	6/1998	Edelstein et al.
5,872,973	A	2/1999	Mitchell et al.
5,913,041	A	6/1999	Ramanathan et al.
5,913,214	A	6/1999	Madnick et al.
6,016,394	A	1/2000	Walker
6,122,627	A	9/2000	Carey et al.
6,148,297	A	11/2000	Swor et al.
6,148,342	A	11/2000	Ho
6,240,416	B1	5/2001	Immon et al.
6,240,422	B1	5/2001	Atkins et al.
6,243,816	B1	6/2001	Fang et al.
6,253,203	B1	6/2001	Oflaherty et al.
6,263,335	B1	7/2001	Paik et al.
6,272,631	B1	8/2001	Thomlinson et al.
6,275,824	B1	8/2001	Oflaherty et al.
6,282,548	B1	8/2001	Burner et al.
6,330,562	B1	12/2001	Boden et al.
6,363,488	B1	3/2002	Ginter et al.
6,374,237	B1	4/2002	Reese
6,374,252	B1	4/2002	Althoff et al.
6,408,336	B1	6/2002	Schneider et al.
6,427,230	B1	7/2002	Goiffon et al.
6,430,556	B1	8/2002	Goldberg et al.
6,442,688	B1	8/2002	Moses et al.
6,446,120	B1	9/2002	Dantressangle
6,463,488	B1	10/2002	San Juan
6,484,149	B1	11/2002	Jammes et al.
6,484,180	B1	11/2002	Lyons et al.
6,516,314	B1	2/2003	Birkler et al.
6,516,337	B1	2/2003	Tripp et al.
6,519,571	B1	2/2003	Guheen et al.
6,574,631	B1	6/2003	Subramanian et al.
6,591,272	B1	7/2003	Williams
6,601,233	B1	7/2003	Underwood
6,606,744	B1	8/2003	Mikurak
6,611,812	B2	8/2003	Hurtado et al.
6,625,602	B1	9/2003	Meredith et al.
6,629,081	B1	9/2003	Cornelius et al.
6,633,878	B1	10/2003	Underwood
6,662,192	B1	12/2003	Rebane
6,662,357	B1	12/2003	Bowman-Amuah
6,697,824	B1	2/2004	Bowman-Amuah
6,699,042	B2	3/2004	Smith et al.
6,701,314	B1	3/2004	Conover et al.
6,721,713	B1	4/2004	Guheen et al.
6,725,200	B1	4/2004	Rost
6,732,109	B2	5/2004	Lindberg et al.
6,754,665	B1	6/2004	Futagami et al.
6,755,344	B1	6/2004	Mollett et al.
6,757,685	B2	6/2004	Raffaele et al.
6,757,888	B1	6/2004	Knutson et al.
6,816,944	B2	11/2004	Peng
6,826,693	B1	11/2004	Yoshida et al.
6,850,252	B1	2/2005	Hoffberg
6,886,101	B2	4/2005	Glazer et al.
6,901,346	B2	5/2005	Tracy et al.
6,904,417	B2	6/2005	Clayton et al.
6,909,897	B2	6/2005	Kikuchi
6,925,443	B1	8/2005	Baggett, Jr. et al.
6,938,041	B1	8/2005	Brandow et al.
6,956,845	B2	10/2005	Baker et al.
6,957,261	B2	10/2005	Lortz
6,978,270	B1	12/2005	Carty et al.
6,980,927	B2	12/2005	Tracy et al.
6,980,987	B2	12/2005	Kaminer
6,983,221	B2	1/2006	Tracy et al.
6,985,887	B1	1/2006	Sunstein et al.
6,990,454	B2	1/2006	McIntosh
6,993,448	B2	1/2006	Tracy et al.
6,993,495	B2	1/2006	Smith, Jr. et al.
6,996,807	B1	2/2006	Vardi et al.
7,003,560	B1	2/2006	Mullen et al.
7,003,662	B2	2/2006	Genty et al.
7,013,290	B2	3/2006	Ananian
7,017,105	B2	3/2006	Flanagin et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,023,979 B1 4/2006 Wu et al.
7,039,594 B1 5/2006 Gersting
7,039,654 B1 5/2006 Eder
7,047,517 B1 5/2006 Brown et al.
7,051,036 B2 5/2006 Rosnow et al.
7,051,038 B1 5/2006 Yeh et al.
7,058,970 B2 6/2006 Shaw
7,069,427 B2 6/2006 Adler et al.
7,076,558 B1 7/2006 Dunn
7,093,200 B2 8/2006 Schreiber et al.
7,093,283 B1 8/2006 Chen et al.
7,095,854 B1 8/2006 Ginter et al.
7,100,195 B1 8/2006 Underwood
7,120,800 B2 10/2006 Ginter et al.
7,124,101 B1 10/2006 Mikurak
7,124,107 B1 10/2006 Pishevar et al.
7,127,705 B2 10/2006 Christfort et al.
7,127,741 B2 10/2006 Bandini et al.
7,133,845 B1 11/2006 Ginter et al.
7,139,999 B2 11/2006 Bowman-Amuah
7,143,091 B2 11/2006 Charnock et al.
7,149,698 B2 12/2006 Guheen et al.
7,165,041 B1 1/2007 Guheen et al.
7,167,842 B1 1/2007 Josephson, II et al.
7,167,844 B1 1/2007 Leong et al.
7,171,379 B2 1/2007 Menninger et al.
7,181,438 B1 2/2007 Szabo
7,188,252 B1 3/2007 Dunn
7,203,929 B1 4/2007 Vinodkrishnan et al.
7,213,233 B1 5/2007 Vinodkrishnan et al.
7,216,232 B1 5/2007 Cox et al.
7,216,340 B1 5/2007 Vinodkrishnan et al.
7,219,066 B2 5/2007 Parks et al.
7,223,234 B2 5/2007 Stupp et al.
7,225,460 B2 5/2007 Barzilai et al.
7,234,065 B2 6/2007 Breslin et al.
7,247,625 B2 7/2007 Zhang et al.
7,251,624 B1 7/2007 Lee et al.
7,260,830 B2 8/2007 Sugimoto
7,266,566 B1 9/2007 Kennaley et al.
7,272,818 B2 9/2007 Ishimitsu et al.
7,275,063 B2 9/2007 Horn
7,281,020 B2 10/2007 Fine
7,284,232 B1 10/2007 Bates et al.
7,284,271 B2 10/2007 Lucovsky et al.
7,287,280 B2 10/2007 Young
7,290,275 B2 10/2007 Baudoin et al.
7,293,119 B2 11/2007 Beale
7,299,299 B2 11/2007 Hollenbeck et al.
7,302,569 B2 11/2007 Betz et al.
7,313,575 B2 12/2007 Carr et al.
7,313,699 B2 12/2007 Koga
7,313,825 B2 12/2007 Redlich et al.
7,315,826 B1 1/2008 Guheen et al.
7,315,849 B2 1/2008 Bakalash et al.
7,322,047 B2 1/2008 Redlich et al.
7,330,850 B1 2/2008 Seibel et al.
7,340,447 B2 3/2008 Ghatare
7,340,776 B2 3/2008 Zobel et al.
7,343,434 B2 3/2008 Kapoor et al.
7,346,518 B1 3/2008 Frank et al.
7,353,204 B2 4/2008 Liu
7,353,281 B2 4/2008 New, Jr. et al.
7,353,283 B2 4/2008 Henaff et al.
7,356,559 B1 4/2008 Jacobs et al.
7,367,014 B2 4/2008 Griffin
7,370,025 B1 5/2008 Pandit
7,376,835 B2 5/2008 Olkin et al.
7,380,120 B1 5/2008 Garcia
7,382,903 B2 6/2008 Ray
7,383,570 B2 6/2008 Pinkas et al.
7,391,854 B2 6/2008 Salonen et al.
7,392,546 B2 6/2008 Patrick
7,398,393 B2 7/2008 Mont et al.
7,401,235 B2 7/2008 Mowers et al.
7,403,942 B1 7/2008 Bayliss
7,409,354 B2 8/2008 Putnam et al.
7,412,402 B2 8/2008 Cooper
7,424,680 B2 9/2008 Carpenter
7,428,546 B2 9/2008 Nori et al.
7,428,707 B2 9/2008 Quimby
7,430,585 B2 9/2008 Sibert
7,454,457 B1 11/2008 Lowery et al.
7,454,508 B2 11/2008 Mathew et al.
7,478,157 B2 1/2009 Bohrer et al.
7,480,694 B2 1/2009 Blennerhassett et al.
7,480,755 B2 1/2009 Herrell et al.
7,487,170 B2 2/2009 Stevens
7,493,282 B2 2/2009 Manly et al.
7,500,607 B2 3/2009 Williams
7,506,248 B2 3/2009 Xu et al.
7,512,987 B2 3/2009 Williams
7,516,882 B2 4/2009 Cucinotta
7,523,053 B2 4/2009 Pudhukottai et al.
7,529,836 B1 5/2009 Bolen
7,548,968 B1 6/2009 Bura et al.
7,552,480 B1 6/2009 Voss
7,562,339 B2 7/2009 Racca et al.
7,565,685 B2 7/2009 Ross et al.
7,567,541 B2 7/2009 Karimi et al.
7,584,505 B2 9/2009 Mondri et al.
7,584,508 B1 9/2009 Kashchenko et al.
7,587,749 B2 9/2009 Leser et al.
7,590,705 B2 9/2009 Mathew et al.
7,590,972 B2 9/2009 Axelrod et al.
7,603,356 B2 10/2009 Schran et al.
7,606,783 B1 10/2009 Carter
7,606,790 B2 10/2009 Levy
7,607,120 B2 10/2009 Sanyal et al.
7,610,391 B2 10/2009 Dunn
7,613,700 B1 11/2009 Lobo et al.
7,617,136 B1 11/2009 Lessing et al.
7,617,167 B2 11/2009 Griffis et al.
7,620,644 B2 11/2009 Cote et al.
7,627,666 B1 12/2009 Degiulio et al.
7,630,874 B2 12/2009 Fables et al.
7,630,998 B2 12/2009 Zhou et al.
7,636,742 B1 12/2009 Olavarrieta et al.
7,640,322 B2 12/2009 Wendkos et al.
7,650,497 B2 1/2010 Thornton et al.
7,653,592 B1 1/2010 Flaxman et al.
7,657,476 B2 2/2010 Barney
7,657,694 B2 2/2010 Mansell et al.
7,665,073 B2 2/2010 Meijer et al.
7,665,125 B2 2/2010 Heard et al.
7,668,947 B2 2/2010 Hutchinson et al.
7,673,282 B2 3/2010 Amaru et al.
7,676,034 B1 3/2010 Wu et al.
7,681,034 B1 3/2010 Lee et al.
7,681,140 B2 3/2010 Ebert
7,685,561 B2 3/2010 Deem et al.
7,685,577 B2 3/2010 Pace et al.
7,693,593 B2 4/2010 Ishibashi et al.
7,698,398 B1 4/2010 Lai
7,702,639 B2 4/2010 Stanley et al.
7,707,224 B2 4/2010 Chastagnol et al.
7,712,029 B2 5/2010 Ferreira et al.
7,716,242 B2 5/2010 Pae et al.
7,725,474 B2 5/2010 Tamai et al.
7,725,875 B2 5/2010 Waldrep
7,729,940 B2 6/2010 Harvey et al.
7,730,142 B2 6/2010 Levasseur et al.
7,735,036 B2 6/2010 Dennison et al.
7,752,124 B2 7/2010 Green et al.
7,756,826 B2 7/2010 Bots et al.
7,756,987 B2 7/2010 Wang et al.
7,761,586 B2 7/2010 Olenick et al.
7,774,745 B2 8/2010 Fildebrandt et al.
7,788,212 B2 8/2010 Beckmann et al.
7,788,222 B2 8/2010 Shah et al.
7,788,632 B2 8/2010 Kuester et al.
7,788,726 B2 8/2010 Teixeira
7,793,318 B2 9/2010 Deng
7,797,726 B2 9/2010 Ashley et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,801,758 B2 9/2010 Gracie et al.
7,801,765 B2 9/2010 Denny
7,801,826 B2 9/2010 Labrou et al.
7,801,912 B2 9/2010 Ransil et al.
7,802,305 B1 9/2010 Leeds
7,805,349 B2 9/2010 Yu et al.
7,805,451 B2 9/2010 Hosokawa
7,813,947 B2 10/2010 Deangelis et al.
7,822,620 B2 10/2010 Dixon et al.
7,827,523 B2 11/2010 Ahmed et al.
7,836,078 B2 11/2010 Dettinger et al.
7,844,640 B2 11/2010 Bender et al.
7,849,143 B2 12/2010 Vuong
7,853,468 B2 12/2010 Callahan et al.
7,853,470 B2 12/2010 Sonnleithner et al.
7,853,925 B2 12/2010 Kemmler
7,860,816 B2 12/2010 Fokoue-Nkoutche et al.
7,870,540 B2 1/2011 Zare et al.
7,870,608 B2 1/2011 Shraim et al.
7,873,541 B1 1/2011 Klar et al.
7,877,327 B2 1/2011 Gwiazda et al.
7,877,812 B2 1/2011 Koved et al.
7,885,841 B2 2/2011 King
7,890,461 B2 2/2011 Oeda et al.
7,895,260 B2 2/2011 Archer et al.
7,904,478 B2 3/2011 Yu et al.
7,904,487 B2 3/2011 Ghatare
7,917,888 B2 3/2011 Chong et al.
7,917,963 B2 3/2011 Goyal et al.
7,921,152 B2 4/2011 Ashley et al.
7,930,197 B2 4/2011 Ozzie et al.
7,930,753 B2 4/2011 Mellinger et al.
7,941,443 B1 5/2011 Sobel et al.
7,953,725 B2 5/2011 Burris et al.
7,954,150 B2 5/2011 Croft et al.
7,958,087 B2 6/2011 Blumenau
7,958,494 B2 6/2011 Chaar et al.
7,962,900 B2 6/2011 Barraclough et al.
7,966,310 B2 6/2011 Sullivan et al.
7,966,599 B1 6/2011 Malasky et al.
7,966,663 B2 6/2011 Strickland et al.
7,974,992 B2 7/2011 Fastabend et al.
7,975,000 B2 7/2011 Dixon et al.
7,991,559 B2 8/2011 Dzekunov et al.
7,991,747 B1 8/2011 Upadhyay et al.
7,996,372 B2 8/2011 Rubel, Jr.
8,005,891 B2 8/2011 Knowles et al.
8,010,612 B2 8/2011 Costea et al.
8,010,720 B2 8/2011 Iwaoka et al.
8,019,881 B2 9/2011 Sandhu et al.
8,020,206 B2 9/2011 Hubbard et al.
8,024,384 B2 9/2011 Prabhakar et al.
8,032,721 B2 10/2011 Murai
8,036,374 B2 10/2011 Noble, Jr.
8,037,409 B2 10/2011 Jacob et al.
8,041,749 B2 10/2011 Beck
8,041,763 B2 10/2011 Kordun et al.
8,041,913 B2 10/2011 Wang
8,069,161 B2 11/2011 Bugir et al.
8,069,471 B2 11/2011 Boren
8,082,539 B1 12/2011 Schelkogonov
8,090,754 B2 1/2012 Schmidt et al.
8,095,923 B2 1/2012 Harvey et al.
8,099,709 B2 1/2012 Baikov et al.
8,103,962 B2 1/2012 Embley et al.
8,117,441 B2 2/2012 Kurien et al.
8,135,815 B2 3/2012 Mayer
8,146,054 B2 3/2012 Baker et al.
8,146,074 B2 3/2012 Ito et al.
8,150,717 B2 4/2012 Whitmore
8,156,105 B2 4/2012 Altounian et al.
8,156,158 B2 4/2012 Rolls et al.
8,156,159 B2 4/2012 Ebrahimi et al.
8,166,406 B1 4/2012 Goldfeder et al.
8,176,061 B2 5/2012 Swanbeck et al.
8,176,177 B2 5/2012 Sussman et al.
8,176,334 B2 5/2012 Vainstein
8,176,470 B2 5/2012 Klumpp et al.
8,180,759 B2 5/2012 Hamzy
8,181,151 B2 5/2012 Sedukhin et al.
8,185,409 B2 5/2012 Putnam et al.
8,195,489 B2 6/2012 Bhamidipaty et al.
8,196,176 B2 6/2012 Berteau et al.
8,205,093 B2 6/2012 Argott
8,205,140 B2 6/2012 Hafeez et al.
8,214,362 B1 7/2012 Djabarov
8,214,803 B2 7/2012 Horii et al.
8,234,133 B2 7/2012 Smith
8,234,145 B2 7/2012 Kissner et al.
8,234,377 B2 7/2012 Cohn
8,239,244 B2 8/2012 Ginsberg et al.
8,250,051 B2 8/2012 Bugir et al.
8,255,468 B2 8/2012 Vitaldevara et al.
8,260,262 B2 9/2012 Ben Ayed
8,261,362 B2 9/2012 Goodwin et al.
8,266,231 B1 9/2012 Golovin et al.
8,275,632 B2 9/2012 Awaraji et al.
8,275,793 B2 9/2012 Ahmad et al.
8,286,239 B1 10/2012 Sutton
8,312,549 B2 11/2012 Goldberg et al.
8,316,237 B1 11/2012 Felsher et al.
8,327,141 B2 12/2012 Vysogorets et al.
8,332,908 B2 12/2012 Hatakeyama et al.
8,340,999 B2 12/2012 Kumaran et al.
8,341,405 B2 12/2012 Meijer et al.
8,346,852 B2 1/2013 Sugasaki
8,346,929 B1 1/2013 Lai
8,364,713 B2 1/2013 Pollard
8,370,224 B2 2/2013 Grewal
8,370,794 B2 2/2013 Moosmann et al.
8,380,630 B2 2/2013 Felsher
8,380,743 B2 2/2013 Convertino et al.
8,381,180 B2 2/2013 Rostoker
8,381,297 B2 2/2013 Touboul
8,386,314 B2 2/2013 Kirkby et al.
8,392,982 B2 3/2013 Harris et al.
8,418,226 B2 4/2013 Gardner
8,423,954 B2 4/2013 Ronen et al.
8,429,179 B1 4/2013 Mirhaji
8,429,597 B2 4/2013 Prigge
8,429,630 B2 4/2013 Nickolov et al.
8,429,758 B2 4/2013 Chen et al.
8,438,644 B2 5/2013 Watters et al.
8,452,693 B2 5/2013 Shah et al.
8,463,247 B2 6/2013 Misiag
8,464,311 B2 6/2013 Ashley et al.
8,468,244 B2 6/2013 Redlich et al.
8,473,324 B2 6/2013 Alvarez et al.
8,474,012 B2 6/2013 Ahmed et al.
8,494,894 B2 7/2013 Jaster et al.
8,504,481 B2 8/2013 Motahari et al.
8,510,199 B1 8/2013 Erlanger
8,515,988 B2 8/2013 Jones et al.
8,516,076 B2 8/2013 Thomas
8,526,922 B1 9/2013 Koster
8,527,337 B1 9/2013 Lim et al.
8,533,746 B2 9/2013 Nolan et al.
8,533,844 B2 9/2013 Mahaffey et al.
8,538,817 B2 9/2013 Wilson
8,539,359 B2 9/2013 Rapaport et al.
8,539,437 B2 9/2013 Finlayson et al.
8,560,645 B2 10/2013 Linden et al.
8,560,841 B2 10/2013 Chin et al.
8,560,956 B2 10/2013 Curtis et al.
8,561,100 B2 10/2013 Hu et al.
8,561,153 B2 10/2013 Grason et al.
8,565,729 B2 10/2013 Moseler et al.
8,566,726 B2 10/2013 Dixon et al.
8,566,938 B1 10/2013 Prakash et al.
8,571,909 B2 10/2013 Miller et al.
8,572,717 B2 10/2013 Narayanaswamy
8,578,036 B1 11/2013 Holfelder et al.
8,578,166 B2 11/2013 De Monseignat et al.
8,578,481 B2 11/2013 Rowley

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,578,501 B1 11/2013 Ogilvie
8,583,694 B2 11/2013 Siegel et al.
8,583,766 B2 11/2013 Dixon et al.
8,589,183 B2 11/2013 Awaraji et al.
8,601,467 B2 12/2013 Hofhansl et al.
8,601,591 B2 12/2013 Krishnamurthy et al.
8,606,746 B2 12/2013 Yeap et al.
8,612,420 B2 12/2013 Sun et al.
8,612,993 B2 12/2013 Grant et al.
8,615,549 B2 12/2013 Knowles et al.
8,615,731 B2 12/2013 Doshi
8,620,952 B2 12/2013 Bennett et al.
8,621,637 B2 12/2013 Al-Harbi et al.
8,626,671 B2 1/2014 Federgreen
8,627,114 B2 1/2014 Resch et al.
8,630,961 B2 1/2014 Beilby et al.
8,631,048 B1 1/2014 Davis et al.
8,640,110 B2 1/2014 Kopp et al.
8,646,072 B1 2/2014 Savant
8,650,399 B2 2/2014 Le Bihan et al.
8,655,939 B2 2/2014 Redlich et al.
8,656,265 B1 2/2014 Paulin et al.
8,656,456 B2 2/2014 Maxson et al.
8,661,036 B2 2/2014 Turski et al.
8,667,074 B1 3/2014 Farkas
8,667,487 B1 3/2014 Boodman et al.
8,677,472 B1 3/2014 Dotan et al.
8,681,984 B2 3/2014 Lee et al.
8,682,698 B2 3/2014 Cashman et al.
8,683,502 B2 3/2014 Shkedi et al.
8,688,601 B2 4/2014 Jaiswal
8,689,292 B2 4/2014 Williams et al.
8,693,689 B2 4/2014 Belenkiy et al.
8,700,524 B2 4/2014 Williams et al.
8,700,699 B2 4/2014 Shen et al.
8,706,742 B1 4/2014 Ravid et al.
8,707,451 B2 4/2014 Ture et al.
8,712,813 B2 4/2014 King
8,713,098 B1 4/2014 Adya et al.
8,713,638 B2 4/2014 Hu et al.
8,719,366 B2 5/2014 Mathew et al.
8,719,421 B2 5/2014 Mao et al.
8,732,839 B2 5/2014 Hohl
8,744,894 B2 6/2014 Christiansen et al.
8,751,285 B2 6/2014 Deb et al.
8,762,406 B2 6/2014 Ho et al.
8,762,413 B2 6/2014 Graham, Jr. et al.
8,763,071 B2 6/2014 Sinha et al.
8,763,082 B2 6/2014 Huber et al.
8,763,131 B2 6/2014 Archer et al.
8,767,947 B1 7/2014 Ristock et al.
8,769,242 B2 7/2014 Tkac et al.
8,769,412 B2 7/2014 Gill et al.
8,769,671 B2 7/2014 Shraim et al.
8,776,241 B2 7/2014 Zaitsev
8,788,935 B1 7/2014 Hirsch et al.
8,793,614 B2 7/2014 Wilson et al.
8,793,650 B2 7/2014 Hilerio et al.
8,793,781 B2 7/2014 Grossi et al.
8,793,809 B2 7/2014 Falkenburg et al.
8,799,984 B2 8/2014 Ahn
8,805,707 B2 8/2014 Schumann, Jr. et al.
8,805,806 B2 8/2014 Amarendran et al.
8,805,925 B2 8/2014 Price et al.
8,812,342 B2 8/2014 Barcelo et al.
8,812,752 B1 8/2014 Shih et al.
8,812,766 B2 8/2014 Kranendonk et al.
8,813,028 B2 8/2014 Farooqi
8,813,177 B2 8/2014 Srour et al.
8,813,214 B1 8/2014 McNair et al.
8,819,253 B2 8/2014 Simeloff et al.
8,819,617 B1 8/2014 Koenig et al.
8,819,800 B2 8/2014 Gao et al.
8,826,446 B1 9/2014 Liu et al.
8,832,649 B2 9/2014 Bishop et al.
8,832,854 B1 9/2014 Staddon et al.
8,839,232 B2 9/2014 Taylor et al.
8,843,487 B2 9/2014 McGraw et al.
8,843,745 B2 9/2014 Roberts, Jr.
8,849,757 B2 9/2014 Kruglick
8,856,534 B2 10/2014 Khosravi et al.
8,856,936 B2 10/2014 Datta Ray et al.
8,862,507 B2 10/2014 Sandhu et al.
8,863,261 B2 10/2014 Yang
8,875,232 B2 10/2014 Blom et al.
8,893,078 B2 11/2014 Schaude et al.
8,893,286 B1 11/2014 Oliver
8,893,297 B2 11/2014 Eversoll et al.
8,904,494 B2 12/2014 Kindler et al.
8,914,263 B2 12/2014 Shimada et al.
8,914,299 B2 12/2014 Pesci-Anderson et al.
8,914,342 B2 12/2014 Kalaboukis et al.
8,914,888 B1 12/2014 Satish et al.
8,914,902 B2 12/2014 Moritz et al.
8,918,306 B2 12/2014 Cashman et al.
8,918,392 B1 12/2014 Brooker et al.
8,918,632 B1 12/2014 Sartor
8,924,388 B2 12/2014 Elliot et al.
8,930,896 B1 1/2015 Wiggins
8,930,897 B2 1/2015 Nassar
8,935,198 B1 1/2015 Phillips et al.
8,935,266 B2 1/2015 Wu
8,935,342 B2 1/2015 Patel
8,935,804 B1 1/2015 Clark et al.
8,938,221 B2 1/2015 Brazier et al.
8,943,076 B2 1/2015 Stewart et al.
8,943,548 B2 1/2015 Drokov et al.
8,943,602 B2 1/2015 Roy et al.
8,949,137 B2 2/2015 Crapo et al.
8,955,038 B2 2/2015 Nicodemus et al.
8,959,568 B2 2/2015 Hudis et al.
8,959,584 B2 2/2015 Piliouras
8,966,575 B2 2/2015 McQuay et al.
8,966,597 B1 2/2015 Saylor et al.
8,973,108 B1 3/2015 Roth et al.
8,977,234 B2 3/2015 Chava
8,977,643 B2 3/2015 Schindlauer et al.
8,978,158 B2 3/2015 Rajkumar et al.
8,983,972 B2 3/2015 Kriebel et al.
8,984,031 B1 3/2015 Todd
8,990,933 B1 3/2015 Magdalin
8,996,417 B1 3/2015 Channakeshava
8,996,480 B2 3/2015 Agarwala et al.
8,997,213 B2 3/2015 Papakipos et al.
9,001,673 B2 4/2015 Birdsall et al.
9,003,295 B2 4/2015 Baschy
9,003,552 B2 4/2015 Goodwin et al.
9,009,851 B2 4/2015 Droste et al.
9,014,661 B2 4/2015 Decharms
9,015,796 B1 4/2015 Fujioka
9,021,469 B2 4/2015 Hilerio et al.
9,026,526 B1 5/2015 Bau et al.
9,030,987 B2 5/2015 Bianchetti et al.
9,032,067 B2 5/2015 Prasad et al.
9,043,217 B2 5/2015 Cashman et al.
9,043,480 B2 5/2015 Barton et al.
9,047,463 B2 6/2015 Porras
9,047,582 B2 6/2015 Hutchinson et al.
9,047,583 B2 6/2015 Patton et al.
9,047,639 B1 6/2015 Quintiliani et al.
9,049,244 B2 6/2015 Prince et al.
9,049,314 B2 6/2015 Pugh et al.
9,055,071 B1 6/2015 Gates et al.
9,058,590 B2 6/2015 Criddle et al.
9,064,033 B2 6/2015 Jin et al.
9,069,940 B2 6/2015 Hars
9,076,231 B1 7/2015 Hill et al.
9,077,736 B2 7/2015 Werth et al.
9,081,952 B2 7/2015 Sagi et al.
9,087,090 B1 7/2015 Cormier et al.
9,092,796 B2 7/2015 Eversoll et al.
9,094,434 B2 7/2015 Williams et al.
9,098,515 B2 8/2015 Richter et al.
9,100,337 B1 8/2015 Battré et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,100,778 B2 8/2015 Stogaitis et al.
9,106,691 B1 8/2015 Burger et al.
9,106,710 B1 8/2015 Feimster
9,110,918 B1 8/2015 Rajaa et al.
9,111,105 B2 8/2015 Barton et al.
9,111,295 B2 8/2015 Tietzen et al.
9,123,330 B1 9/2015 Sharifi et al.
9,123,339 B1 9/2015 Shaw et al.
9,129,311 B2 9/2015 Schoen et al.
9,135,261 B2 9/2015 Maunder et al.
9,135,444 B2 9/2015 Carter et al.
9,141,823 B2 9/2015 Dawson
9,141,911 B2 9/2015 Zhao et al.
9,152,818 B1 10/2015 Hathaway et al.
9,152,820 B1 10/2015 Pauley, Jr. et al.
9,154,514 B1 10/2015 Prakash
9,154,556 B1 10/2015 Dotan et al.
9,158,655 B2 10/2015 Wadhwani et al.
9,165,036 B2 10/2015 Mehra
9,170,996 B2 10/2015 Lovric et al.
9,172,706 B2 10/2015 Krishnamurthy et al.
9,177,293 B1 11/2015 Gagnon et al.
9,178,901 B2 11/2015 Xue et al.
9,183,100 B2 11/2015 Gventer et al.
9,189,642 B2 11/2015 Perlman
9,201,572 B2 12/2015 Lyon et al.
9,201,770 B1 12/2015 Duerk
9,202,026 B1 12/2015 Reeves
9,202,085 B2 12/2015 Mawdsley et al.
9,215,076 B1 12/2015 Roth et al.
9,215,252 B2 12/2015 Smith et al.
9,218,596 B2 12/2015 Ronca et al.
9,224,009 B1 12/2015 Liu et al.
9,230,036 B2 1/2016 Davis
9,231,935 B1 1/2016 Bridge et al.
9,232,040 B2 1/2016 Barash et al.
9,235,476 B2 1/2016 McHugh et al.
9,240,987 B2 1/2016 Barrett-Bowen et al.
9,241,259 B2 1/2016 Daniela et al.
9,245,126 B2 1/2016 Christodorescu et al.
9,245,266 B2 1/2016 Hardt
9,253,609 B2 2/2016 Hosier, Jr.
9,264,443 B2 2/2016 Weisman
9,274,858 B2 3/2016 Milliron et al.
9,280,581 B1 3/2016 Grimes et al.
9,286,149 B2 3/2016 Sampson et al.
9,286,282 B2 3/2016 Ling, III et al.
9,288,118 B1 3/2016 Pattan
9,288,556 B2 3/2016 Kim et al.
9,294,498 B1 3/2016 Yampolskiy et al.
9,299,050 B2 3/2016 Stiffler et al.
9,306,939 B2 4/2016 Chan et al.
9,317,697 B2 4/2016 Maier et al.
9,317,715 B2 4/2016 Schuette et al.
9,325,731 B2 4/2016 McGeehan
9,336,184 B2 5/2016 Mital et al.
9,336,220 B2 5/2016 Li et al.
9,336,324 B2 5/2016 Lomme et al.
9,336,332 B2 5/2016 Davis et al.
9,336,400 B2 5/2016 Milman et al.
9,338,188 B1 5/2016 Ahn
9,342,706 B2 5/2016 Chawla et al.
9,344,297 B2 5/2016 Shah et al.
9,344,424 B2 5/2016 Tenenboym et al.
9,344,484 B2 5/2016 Ferris
9,348,802 B2 5/2016 Massand
9,348,862 B2 5/2016 Kawecki, III
9,348,929 B2 5/2016 Eberlein
9,349,016 B1 5/2016 Brisebois et al.
9,350,718 B2 5/2016 Sondhi et al.
9,355,157 B2 5/2016 Mohammed et al.
9,356,961 B1 5/2016 Todd et al.
9,361,446 B1 6/2016 Demirjian et al.
9,369,488 B2 6/2016 Woods et al.
9,372,869 B2 6/2016 Joseph et al.
9,374,693 B1 6/2016 Olincy et al.
9,384,199 B2 7/2016 Thereska et al.
9,384,357 B2 7/2016 Patil et al.
9,386,078 B2 7/2016 Reno et al.
9,386,104 B2 7/2016 Adams et al.
9,395,959 B2 7/2016 Hatfield et al.
9,396,332 B2 7/2016 Abrams et al.
9,401,900 B2 7/2016 Levasseur et al.
9,411,967 B2 8/2016 Parecki et al.
9,411,982 B1 8/2016 Dippenaar et al.
9,417,859 B2 8/2016 Gounares et al.
9,418,221 B2 8/2016 Turgeman
9,424,021 B2 8/2016 Zamir
9,424,414 B1 8/2016 Demirjian et al.
9,426,177 B2 8/2016 Wang et al.
9,450,940 B2 9/2016 Belov et al.
9,460,136 B1 10/2016 Todd et al.
9,460,171 B2 10/2016 Marrelli et al.
9,460,307 B2 10/2016 Breslau et al.
9,461,876 B2 10/2016 Van Dusen et al.
9,462,009 B1 10/2016 Kolman et al.
9,465,702 B2 10/2016 Gventer et al.
9,465,800 B2 10/2016 Lacey
9,473,446 B2 10/2016 Vijay et al.
9,473,505 B1 10/2016 Asano et al.
9,473,535 B2 10/2016 Sartor
9,477,523 B1 10/2016 Warman et al.
9,477,660 B2 10/2016 Scott et al.
9,477,685 B1 10/2016 Leung et al.
9,477,942 B2 10/2016 Adachi et al.
9,483,659 B2 11/2016 Bao et al.
9,489,366 B2 11/2016 Scott et al.
9,495,547 B1 11/2016 Schepis et al.
9,501,523 B2 11/2016 Hyatt et al.
9,507,960 B2 11/2016 Bell et al.
9,509,674 B1 11/2016 Nasserbakht et al.
9,509,702 B2 11/2016 Grigg et al.
9,514,231 B2 12/2016 Eden
9,516,012 B2 12/2016 Chochois et al.
9,521,166 B2 12/2016 Wilson
9,524,500 B2 12/2016 Dave et al.
9,529,989 B2 12/2016 Kling et al.
9,536,108 B2 1/2017 Powell et al.
9,537,546 B2 1/2017 Cordeiro et al.
9,542,568 B2 1/2017 Francis et al.
9,549,047 B1 1/2017 Fredinburg et al.
9,552,395 B2 1/2017 Bayer et al.
9,552,470 B2 1/2017 Turgeman et al.
9,553,918 B1 1/2017 Manion et al.
9,558,497 B2 1/2017 Carvalho
9,569,752 B2 2/2017 Deering et al.
9,571,506 B2 2/2017 Boss et al.
9,571,509 B1 2/2017 Satish et al.
9,571,526 B2 2/2017 Sartor
9,571,559 B2 2/2017 Raleigh et al.
9,571,991 B1 2/2017 Brizendine et al.
9,576,289 B2 2/2017 Henderson et al.
9,578,060 B1 2/2017 Brisebois et al.
9,578,173 B2 2/2017 Sanghavi et al.
9,582,681 B2 2/2017 Mishra
9,584,964 B2 2/2017 Pelkey
9,589,110 B2 3/2017 Carey et al.
9,600,181 B2 3/2017 Patel et al.
9,602,529 B2 3/2017 Jones et al.
9,606,971 B2 3/2017 Seolas et al.
9,607,041 B2 3/2017 Himmelstein
9,619,652 B2 4/2017 Slater
9,619,661 B1 4/2017 Finkelstein
9,621,357 B2 4/2017 Williams et al.
9,621,566 B2 4/2017 Gupta et al.
9,626,124 B2 4/2017 Lipinski et al.
9,626,680 B1 4/2017 Ryan et al.
9,629,064 B2 4/2017 Graves et al.
9,642,008 B2 5/2017 Wyatt et al.
9,646,095 B1 5/2017 Gottlieb et al.
9,647,949 B2 5/2017 Varki et al.
9,648,036 B2 5/2017 Seiver et al.
9,652,314 B2 5/2017 Mahiddini
9,654,506 B2 5/2017 Barrett

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,654,541 B1 5/2017 Kapczynski et al.
9,665,722 B2 5/2017 Nagasundaram et al.
9,665,733 B1 5/2017 Sills et al.
9,665,883 B2 5/2017 Roullier et al.
9,672,053 B2 6/2017 Tang et al.
9,672,355 B2 6/2017 Titonis et al.
9,678,794 B1 6/2017 Barrett et al.
9,691,090 B1 6/2017 Barday
9,697,368 B2 7/2017 Dharawat
9,699,209 B2 7/2017 Ng et al.
9,703,549 B2 7/2017 Dufresne
9,704,103 B2 7/2017 Suskind et al.
9,705,840 B2 7/2017 Pujare et al.
9,705,880 B2 7/2017 Siris
9,721,078 B2 8/2017 Cornick et al.
9,721,108 B2 8/2017 Krishnamurthy et al.
9,727,751 B2 8/2017 Oliver et al.
9,729,583 B1 8/2017 Barday
9,734,148 B2 8/2017 Bendersky et al.
9,734,255 B2 8/2017 Jiang
9,736,004 B2 8/2017 Jung et al.
9,740,985 B2 8/2017 Byron et al.
9,740,987 B2 8/2017 Dolan
9,749,408 B2 8/2017 Subramani et al.
9,754,091 B2 9/2017 Kode et al.
9,756,059 B2 9/2017 Demirjian et al.
9,760,620 B2 9/2017 Nachnani et al.
9,760,635 B2 9/2017 Bliss et al.
9,760,697 B1 9/2017 Walker
9,760,849 B2 9/2017 Vinnakota et al.
9,762,553 B2 9/2017 Ford et al.
9,767,202 B2 9/2017 Darby et al.
9,767,309 B1 9/2017 Patel et al.
9,769,124 B2 9/2017 Yan
9,773,269 B1 9/2017 Lazarus
9,785,795 B2 10/2017 Grondin et al.
9,787,671 B1 10/2017 Bogrett
9,798,749 B2 10/2017 Saner
9,798,826 B2 10/2017 Wilson et al.
9,798,896 B2 10/2017 Jakobsson
9,800,605 B2 10/2017 Baikalov et al.
9,800,606 B1 10/2017 Yumer
9,804,649 B2 10/2017 Cohen et al.
9,804,928 B2 10/2017 Davis et al.
9,805,381 B2 10/2017 Frank et al.
9,811,532 B2 11/2017 Parkison et al.
9,817,850 B2 11/2017 Dubbels et al.
9,817,978 B2 11/2017 Marsh et al.
9,819,684 B2 11/2017 Cernoch et al.
9,825,928 B2 11/2017 Lelcuk et al.
9,830,563 B2 11/2017 Paknad
9,832,633 B2 11/2017 Gerber, Jr. et al.
9,836,598 B2 12/2017 Iyer et al.
9,838,407 B1 12/2017 Oprea et al.
9,838,839 B2 12/2017 Vudali et al.
9,841,969 B2 12/2017 Seibert, Jr. et al.
9,842,042 B2 12/2017 Chhatwal et al.
9,842,349 B2 12/2017 Sawczuk et al.
9,848,005 B2 12/2017 Ardeli et al.
9,848,061 B1 12/2017 Jain et al.
9,852,150 B2 12/2017 Sharpe et al.
9,853,959 B1 12/2017 Kapczynski et al.
9,860,226 B2 1/2018 Thormaehlen
9,864,735 B1 1/2018 Lamprecht
9,876,825 B2 1/2018 Amar et al.
9,877,138 B1 1/2018 Franklin
9,880,157 B2 1/2018 Levak et al.
9,882,935 B2 1/2018 Barday
9,887,965 B2 2/2018 Kay et al.
9,888,377 B1 2/2018 McCorkendale et al.
9,892,441 B2 2/2018 Barday
9,892,442 B2 2/2018 Barday
9,892,443 B2 2/2018 Barday
9,892,444 B2 2/2018 Barday
9,894,076 B2 2/2018 Li et al.
9,898,613 B1 2/2018 Swerdlow et al.
9,898,739 B2 2/2018 Monastyrsky et al.
9,898,769 B2 2/2018 Barday
9,912,625 B2 3/2018 Mutha et al.
9,912,677 B2 3/2018 Chien
9,912,810 B2 3/2018 Segre et al.
9,916,703 B2 3/2018 Levinson et al.
9,922,124 B2 3/2018 Rathod
9,923,927 B1 3/2018 McClintock et al.
9,928,379 B1 3/2018 Hoffer
9,934,493 B2 4/2018 Castinado et al.
9,934,544 B1 4/2018 Whitfield et al.
9,936,127 B2 4/2018 Todasco
9,942,214 B1 4/2018 Burciu et al.
9,942,244 B2 4/2018 Lahoz et al.
9,942,276 B2 4/2018 Sartor
9,946,897 B2 4/2018 Lovin
9,948,652 B2 4/2018 Yu et al.
9,948,663 B1 4/2018 Wang et al.
9,953,189 B2 4/2018 Cook et al.
9,954,879 B1 4/2018 Sadaghiani et al.
9,954,883 B2 4/2018 Ahuja et al.
9,959,551 B1 5/2018 Schermerhorn et al.
9,959,582 B2 5/2018 Sukman et al.
9,961,070 B2 5/2018 Tang
9,973,518 B2 5/2018 Lee et al.
9,973,585 B2 5/2018 Ruback et al.
9,977,904 B2 5/2018 Khan et al.
9,977,920 B2 5/2018 Danielson et al.
9,983,936 B2 5/2018 Dornemann et al.
9,984,252 B2 5/2018 Pollard
9,990,499 B2 6/2018 Chan et al.
9,992,213 B2 6/2018 Sinnema
10,001,975 B2 6/2018 Bharthulwar
10,002,064 B2 6/2018 Muske
10,007,895 B2 6/2018 Vanasco
10,013,577 B1 7/2018 Beaumont et al.
10,015,164 B2 7/2018 Hamburg et al.
10,019,339 B2 7/2018 Von Hanxleden et al.
10,019,588 B2 7/2018 Garcia et al.
10,019,591 B1 7/2018 Beguin
10,019,741 B2 7/2018 Hesselink
10,021,143 B2 7/2018 Cabrera et al.
10,025,804 B2 7/2018 Vranyes et al.
10,025,836 B2 7/2018 Batchu et al.
10,028,226 B2 7/2018 Ayyagari et al.
10,032,172 B2 7/2018 Barday
10,044,761 B2 8/2018 Ducatel et al.
10,055,426 B2 8/2018 Arasan et al.
10,055,869 B2 8/2018 Borrelli et al.
10,061,847 B2 8/2018 Mohammed et al.
10,069,858 B2 9/2018 Robinson et al.
10,069,914 B1 9/2018 Smith
10,073,924 B2 9/2018 Karp et al.
10,075,437 B1 9/2018 Costigan et al.
10,075,451 B1 9/2018 Hall et al.
10,084,817 B2 9/2018 Saher et al.
10,091,214 B2 10/2018 Godlewski et al.
10,091,312 B1 10/2018 Khanwalkar et al.
10,097,551 B2 10/2018 Chan et al.
10,102,533 B2 10/2018 Barday
10,108,409 B2 10/2018 Pirzadeh et al.
10,122,663 B2 11/2018 Hu et al.
10,122,760 B2 11/2018 Terrill et al.
10,127,403 B2 11/2018 Kong et al.
10,129,211 B2 11/2018 Heath
10,140,666 B1 11/2018 Wang et al.
10,142,113 B2 11/2018 Zaidi et al.
10,152,560 B2 12/2018 Potiagalov et al.
10,157,269 B2 12/2018 Thomas
10,158,676 B2 12/2018 Barday
10,165,011 B2 12/2018 Barday
10,169,762 B2 1/2019 Ogawa
10,176,503 B2 1/2019 Barday et al.
10,181,043 B1 1/2019 Pauley, Jr. et al.
10,181,051 B2 1/2019 Barday et al.
10,187,363 B2 1/2019 Smirnoff et al.
10,187,394 B2 1/2019 Bar et al.
10,188,950 B2 1/2019 Biswas et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,204,154 B2 2/2019 Barday et al.
10,205,994 B2 2/2019 Splaine et al.
10,210,347 B2 2/2019 McCorkendale et al.
10,212,134 B2 2/2019 Rai
10,212,175 B2 2/2019 Seul et al.
10,223,533 B2 3/2019 Dawson
10,230,571 B2 3/2019 Rangasamy et al.
10,250,594 B2 4/2019 Chathoth et al.
10,255,602 B2 4/2019 Wang
10,257,127 B2 4/2019 Dotan-Cohen et al.
10,257,181 B1 4/2019 Sherif et al.
10,268,838 B2 4/2019 Yadgiri et al.
10,275,221 B2 4/2019 Thattai et al.
10,275,614 B2 4/2019 Barday et al.
10,282,370 B1 5/2019 Barday et al.
10,282,559 B2 5/2019 Barday et al.
10,284,604 B2 5/2019 Barday et al.
10,289,584 B2 5/2019 Chiba
10,289,857 B1 5/2019 Brinskelle
10,289,866 B2 5/2019 Barday et al.
10,289,867 B2 5/2019 Barday et al.
10,289,870 B2 5/2019 Barday et al.
10,296,504 B2 5/2019 Hock et al.
10,304,442 B1 5/2019 Rudden et al.
10,310,723 B2 6/2019 Rathod
10,311,042 B1 6/2019 Kumar
10,311,249 B2 6/2019 Sharifi et al.
10,311,475 B2 6/2019 Yuasa
10,311,492 B2 6/2019 Gelfenbeyn et al.
10,318,761 B2 6/2019 Barday et al.
10,320,940 B1 6/2019 Brennan et al.
10,324,960 B1 6/2019 Skvortsov et al.
10,326,768 B2 6/2019 Verweyst et al.
10,326,798 B2 6/2019 Lambert
10,326,841 B2 6/2019 Bradley et al.
10,331,689 B2 6/2019 Sorrentino et al.
10,331,904 B2 6/2019 Sher-Jan et al.
10,333,975 B2 6/2019 Soman et al.
10,339,470 B1 7/2019 Dutta et al.
10,346,186 B2 7/2019 Kalyanpur
10,346,635 B2 7/2019 Kumar et al.
10,346,637 B2 7/2019 Barday et al.
10,346,638 B2 7/2019 Barday et al.
10,346,849 B2 7/2019 Ionescu et al.
10,348,726 B2 7/2019 Caluwaert
10,348,775 B2 7/2019 Barday
10,353,673 B2 7/2019 Barday et al.
10,361,857 B2 7/2019 Woo
10,366,241 B2 7/2019 Sartor
10,373,119 B2 8/2019 Driscoll et al.
10,373,409 B2 8/2019 White et al.
10,375,115 B2 8/2019 Mallya
10,387,559 B1 8/2019 Wendt et al.
10,387,577 B2 8/2019 Hill et al.
10,387,657 B2 8/2019 Belfiore, Jr. et al.
10,387,952 B1 8/2019 Sandhu et al.
10,395,201 B2 8/2019 Vescio
10,402,545 B2 9/2019 Gorfein et al.
10,404,729 B2 9/2019 Turgeman
10,410,243 B2 9/2019 Boal
10,417,401 B2 9/2019 Votaw et al.
10,417,621 B2 9/2019 Cassel et al.
10,419,476 B2 9/2019 Parekh
10,423,985 B1 9/2019 Dutta et al.
10,425,492 B2 9/2019 Comstock et al.
10,430,608 B2 10/2019 Peri et al.
10,435,350 B2 10/2019 Ito et al.
10,437,412 B2 10/2019 Barday et al.
10,437,860 B2 10/2019 Barday et al.
10,438,016 B2 10/2019 Barday et al.
10,438,273 B2 10/2019 Burns et al.
10,440,062 B2 10/2019 Barday et al.
10,445,508 B2 10/2019 Sher-Jan et al.
10,445,526 B2 10/2019 Barday et al.
10,452,864 B2 10/2019 Barday et al.
10,452,866 B2 10/2019 Barday et al.
10,453,076 B2 10/2019 Parekh et al.
10,453,092 B1 10/2019 Wang et al.
10,454,934 B2 10/2019 Parimi et al.
10,481,763 B2 11/2019 Bartkiewicz et al.
10,489,454 B1 11/2019 Chen
10,503,926 B2 12/2019 Barday et al.
10,509,644 B2 12/2019 Shoavi et al.
10,510,031 B2 12/2019 Barday et al.
10,521,623 B2 12/2019 Rodriguez et al.
10,534,851 B1 1/2020 Chan et al.
10,535,081 B2 1/2020 Ferreira et al.
10,536,475 B1 1/2020 McCorkle, Jr. et al.
10,536,478 B2 1/2020 Kirti et al.
10,540,212 B2 1/2020 Feng et al.
10,541,938 B1 1/2020 Timmerman et al.
10,546,135 B1 1/2020 Kassoumeh et al.
10,552,462 B1 2/2020 Hart
10,558,809 B1 2/2020 Joyce et al.
10,558,821 B2 2/2020 Barday et al.
10,564,815 B2 2/2020 Soon-Shiong
10,564,935 B2 2/2020 Barday et al.
10,564,936 B2 2/2020 Barday et al.
10,565,161 B2 2/2020 Barday et al.
10,565,236 B1 2/2020 Barday et al.
10,567,439 B2 2/2020 Barday
10,567,517 B2 2/2020 Weinig et al.
10,572,684 B2 2/2020 Lafever et al.
10,572,686 B2 2/2020 Barday et al.
10,574,705 B2 2/2020 Barday et al.
10,581,825 B2 3/2020 Poschel et al.
10,592,648 B2 3/2020 Barday et al.
10,592,692 B2 3/2020 Brannon et al.
10,599,456 B2 3/2020 Lissack
10,606,916 B2 3/2020 Brannon et al.
10,613,971 B1 4/2020 Vasikarla
10,614,365 B2 4/2020 Sathish et al.
10,628,553 B1 4/2020 Murrish et al.
10,645,102 B2 5/2020 Hamdi
10,645,548 B2 5/2020 Reynolds et al.
10,649,630 B1 5/2020 Vora et al.
10,650,408 B1 5/2020 Andersen et al.
10,657,469 B2 5/2020 Bade et al.
10,657,504 B1 5/2020 Zimmerman et al.
10,659,566 B1 5/2020 Luah et al.
10,671,749 B2 6/2020 Felice-Steele et al.
10,671,760 B2 6/2020 Esmailzadeh et al.
10,678,945 B2 6/2020 Barday et al.
10,685,140 B2 6/2020 Barday et al.
10,706,176 B2 7/2020 Brannon et al.
10,706,226 B2 7/2020 Byun et al.
10,708,305 B2 7/2020 Barday et al.
10,713,387 B2 7/2020 Brannon et al.
10,726,145 B2 7/2020 Duminy et al.
10,726,153 B2 7/2020 Nerurkar et al.
10,726,158 B2 7/2020 Brannon et al.
10,732,865 B2 8/2020 Jain et al.
10,735,388 B2 8/2020 Rose et al.
10,740,487 B2 8/2020 Barday et al.
10,747,893 B2 8/2020 Kiriyama et al.
10,747,897 B2 8/2020 Cook
10,749,870 B2 8/2020 Brouillette et al.
10,762,213 B2 9/2020 Rudek et al.
10,762,230 B2 9/2020 Ancin et al.
10,762,236 B2 9/2020 Brannon et al.
10,769,302 B2 9/2020 Barday et al.
10,769,303 B2 9/2020 Brannon et al.
10,776,510 B2 9/2020 Antonelli et al.
10,776,518 B2 9/2020 Barday et al.
10,778,792 B1 9/2020 Handy Bosma et al.
10,783,256 B2 9/2020 Brannon et al.
10,785,173 B2 9/2020 Willett et al.
10,785,299 B2 9/2020 Gupta et al.
10,789,594 B2 9/2020 Moshir et al.
10,791,150 B2 9/2020 Barday et al.
10,795,527 B1 10/2020 Legge et al.
10,796,020 B2 10/2020 Barday et al.
10,796,260 B2 10/2020 Brannon et al.
10,798,133 B2 10/2020 Barday et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,803,196 B2 10/2020 Bodegas Martinez et al.
10,805,331 B2 10/2020 Boyer et al.
10,831,831 B2 11/2020 Greene
10,834,590 B2 11/2020 Turgeman et al.
10,846,433 B2 11/2020 Brannon et al.
10,853,356 B1 12/2020 McPherson et al.
10,853,501 B2 12/2020 Brannon
10,860,721 B1 12/2020 Gentile
10,860,742 B2 12/2020 Joseph et al.
10,860,979 B2 12/2020 Geffen et al.
10,878,127 B2 12/2020 Brannon et al.
10,885,485 B2 1/2021 Brannon et al.
10,891,393 B2 1/2021 Currier et al.
10,893,074 B2 1/2021 Sartor
10,896,394 B2 1/2021 Brannon et al.
10,902,490 B2 1/2021 He et al.
10,909,488 B2 2/2021 Hecht et al.
10,924,514 B1 2/2021 Altman et al.
10,929,557 B2 2/2021 Chavez
10,949,555 B2 3/2021 Rattan et al.
10,949,565 B2 3/2021 Barday et al.
10,956,213 B1 3/2021 Chambers et al.
10,957,326 B2 3/2021 Bhaya et al.
10,963,571 B2 3/2021 Bar Joseph et al.
10,963,572 B2 3/2021 Belfiore, Jr. et al.
10,965,547 B1 3/2021 Esposito et al.
10,970,418 B2 4/2021 Durvasula et al.
10,972,509 B2 4/2021 Barday et al.
10,976,950 B1 4/2021 Trezzo et al.
10,981,689 B2 * 4/2021 Altus B65D 1/04
10,983,963 B1 4/2021 Venkatasubramanian et al.
10,984,458 B1 4/2021 Gutierrez
10,997,318 B2 5/2021 Barday et al.
11,003,748 B2 5/2021 Oliker et al.
11,012,475 B2 5/2021 Patnala et al.
11,019,062 B2 5/2021 Chittampally
11,023,528 B1 6/2021 Lee et al.
11,023,921 B2 6/2021 Wang et al.
11,037,168 B1 6/2021 Lee et al.
11,057,356 B2 7/2021 Malhotra et al.
11,057,427 B2 7/2021 Wright et al.
11,062,051 B2 7/2021 Barday et al.
11,068,318 B2 7/2021 Kuesel et al.
11,068,584 B2 7/2021 Burriesci et al.
11,068,618 B2 7/2021 Brannon et al.
11,068,797 B2 7/2021 Bhide et al.
11,068,847 B2 7/2021 Boutros et al.
11,082,499 B2 8/2021 Rivera
11,093,643 B2 8/2021 Hennebert
11,093,950 B2 8/2021 Hersh et al.
11,138,299 B2 10/2021 Brannon et al.
11,144,622 B2 10/2021 Brannon et al.
11,144,678 B2 10/2021 Dondini et al.
11,144,862 B1 10/2021 Jackson et al.
11,195,134 B2 12/2021 Brannon et al.
11,201,929 B2 12/2021 Dudmesh et al.
11,210,420 B2 12/2021 Brannon et al.
11,222,139 B2 1/2022 Jones et al.
11,222,142 B2 1/2022 Jones et al.
11,238,390 B2 2/2022 Brannon et al.
11,240,273 B2 2/2022 Barday et al.
11,246,520 B2 2/2022 Clifford et al.
11,252,159 B2 2/2022 Kannan et al.
11,256,777 B2 2/2022 Brannon et al.
11,263,262 B2 3/2022 Chen
11,327,996 B2 5/2022 Reynolds et al.
11,695,975 B1 7/2023 Giraud
2002/0004736 A1 1/2002 Roundtree et al.
2002/0049907 A1 4/2002 Woods et al.
2002/0055932 A1 5/2002 Wheeler et al.
2002/0077941 A1 6/2002 Halligan et al.
2002/0103854 A1 8/2002 Okita
2002/0129216 A1 9/2002 Collins
2002/0161594 A1 10/2002 Bryan et al.
2002/0161733 A1 10/2002 Grainger
2003/0041250 A1 2/2003 Proudler
2003/0065641 A1 4/2003 Chaloux
2003/0093680 A1 5/2003 Astley et al.
2003/0097451 A1 5/2003 Bjorksten et al.
2003/0097661 A1 5/2003 Li et al.
2003/0115142 A1 6/2003 Brickell et al.
2003/0130893 A1 7/2003 Farmer
2003/0131001 A1 7/2003 Matsuo
2003/0131093 A1 7/2003 Aschen et al.
2003/0140150 A1 7/2003 Kemp et al.
2003/0167216 A1 9/2003 Brown et al.
2003/0212604 A1 11/2003 Cullen
2004/0002818 A1 1/2004 Kulp et al.
2004/0025053 A1 2/2004 Hayward
2004/0088235 A1 5/2004 Ziekle et al.
2004/0098366 A1 5/2004 Sinclair et al.
2004/0098493 A1 5/2004 Rees
2004/0111359 A1 6/2004 Hudock
2004/0186912 A1 9/2004 Harlow et al.
2004/0193907 A1 9/2004 Patanella
2005/0022198 A1 1/2005 Olapurath et al.
2005/0033616 A1 2/2005 Vavul et al.
2005/0076294 A1 4/2005 Dehamer et al.
2005/0114343 A1 5/2005 Wesinger, Jr. et al.
2005/0144066 A1 6/2005 Cope et al.
2005/0197884 A1 9/2005 Mullen, Jr.
2005/0198177 A1 9/2005 Black
2005/0198646 A1 9/2005 Kortela
2005/0246292 A1 11/2005 Sarcanin
2005/0251865 A1 11/2005 Mont et al.
2005/0278538 A1 12/2005 Fowler
2006/0031078 A1 2/2006 Pizzinger et al.
2006/0035204 A1 2/2006 Lamarche et al.
2006/0075122 A1 4/2006 Lindskog et al.
2006/0149730 A1 7/2006 Curtis
2006/0156052 A1 7/2006 Bodnar et al.
2006/0190280 A1 8/2006 Hoebel et al.
2006/0206375 A1 9/2006 Scott et al.
2006/0224422 A1 10/2006 Cohen
2006/0253597 A1 11/2006 Mujica
2006/0259416 A1 11/2006 Johnson
2007/0011058 A1 1/2007 Dev
2007/0027715 A1 2/2007 Gropper et al.
2007/0061125 A1 3/2007 Bhatt et al.
2007/0061393 A1 3/2007 Moore
2007/0130101 A1 6/2007 Anderson et al.
2007/0130323 A1 6/2007 Landsman et al.
2007/0157311 A1 7/2007 Meier et al.
2007/0173355 A1 7/2007 Klein
2007/0179793 A1 8/2007 Bagchi et al.
2007/0180490 A1 8/2007 Renzi et al.
2007/0192438 A1 8/2007 Goei
2007/0266420 A1 11/2007 Hawkins et al.
2007/0283171 A1 12/2007 Breslin et al.
2008/0005194 A1 1/2008 Smolen et al.
2008/0015927 A1 1/2008 Ramirez
2008/0028065 A1 1/2008 Caso et al.
2008/0028435 A1 1/2008 Strickland et al.
2008/0047016 A1 2/2008 Spoonamore
2008/0120699 A1 5/2008 Spear
2008/0140696 A1 6/2008 Mathuria
2008/0189306 A1 8/2008 Hewett et al.
2008/0195436 A1 8/2008 Whyte
2008/0222271 A1 9/2008 Spires
2008/0235177 A1 9/2008 Kim et al.
2008/0270203 A1 10/2008 Holmes et al.
2008/0270351 A1 10/2008 Thomsen
2008/0270381 A1 10/2008 Thomsen
2008/0270382 A1 10/2008 Thomsen et al.
2008/0270451 A1 10/2008 Thomsen et al.
2008/0270462 A1 10/2008 Thomsen
2008/0281649 A1 11/2008 Morris
2008/0282320 A1 11/2008 Denovo et al.
2008/0288271 A1 11/2008 Faust
2008/0288299 A1 11/2008 Schultz
2009/0012896 A1 1/2009 Arnold
2009/0022301 A1 1/2009 Mudaliar
2009/0037975 A1 2/2009 Ishikawa et al.
2009/0119500 A1 5/2009 Roth et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0132419 A1 5/2009 Grammer et al.
2009/0138276 A1 5/2009 Hayashida et al.
2009/0140035 A1 6/2009 Miller
2009/0144702 A1 6/2009 Atkin et al.
2009/0158249 A1 6/2009 Tomkins et al.
2009/0172705 A1 7/2009 Cheong
2009/0182818 A1 7/2009 Krywaniuk
2009/0187764 A1 7/2009 Astakhov et al.
2009/0204452 A1 8/2009 Iskandar et al.
2009/0204820 A1 8/2009 Brandenburg et al.
2009/0210347 A1 8/2009 Sarcanin
2009/0216610 A1 8/2009 Chorny
2009/0249076 A1 10/2009 Reed et al.
2009/0303237 A1 12/2009 Liu et al.
2010/0010912 A1 1/2010 Jones et al.
2010/0010968 A1 1/2010 Redlich et al.
2010/0077484 A1 3/2010 Paretti et al.
2010/0082533 A1 4/2010 Nakamura et al.
2010/0094650 A1 4/2010 Tran et al.
2010/0100398 A1 4/2010 Auker et al.
2010/0121773 A1 5/2010 Currier et al.
2010/0192201 A1 7/2010 Shimoni et al.
2010/0205057 A1 8/2010 Hook et al.
2010/0223349 A1 9/2010 Thorson
2010/0228786 A1 9/2010 Török
2010/0234987 A1 9/2010 Benschop et al.
2010/0235297 A1 9/2010 Mamorsky
2010/0235915 A1 9/2010 Memon et al.
2010/0262624 A1 10/2010 Pullikottil
2010/0268628 A1 10/2010 Pitkow et al.
2010/0268932 A1 10/2010 Bhattacharjee
2010/0281313 A1 11/2010 White et al.
2010/0287114 A1 11/2010 Bartko et al.
2010/0333012 A1 12/2010 Adachi et al.
2011/0006996 A1 1/2011 Smith et al.
2011/0010202 A1 1/2011 Neale
2011/0082794 A1 4/2011 Blechman
2011/0137696 A1 6/2011 Meyer et al.
2011/0145154 A1 6/2011 Rivers et al.
2011/0153396 A1 6/2011 Marcuvitz et al.
2011/0191664 A1 8/2011 Sheleheda et al.
2011/0208850 A1 8/2011 Sheleheda et al.
2011/0209067 A1 8/2011 Bogess et al.
2011/0231896 A1 9/2011 Tovar
2011/0238573 A1 9/2011 Varadarajan
2011/0252456 A1 10/2011 Hatakeyama
2011/0287748 A1 11/2011 Angel et al.
2011/0302643 A1 12/2011 Pichna et al.
2012/0041939 A1 2/2012 Amsterdamski
2012/0084151 A1 4/2012 Kozak et al.
2012/0084349 A1 4/2012 Lee et al.
2012/0102411 A1 4/2012 Sathish
2012/0102543 A1 4/2012 Kohli et al.
2012/0109830 A1 5/2012 Vogel
2012/0110674 A1 5/2012 Belani et al.
2012/0116923 A1 5/2012 Irving et al.
2012/0131438 A1 5/2012 Li et al.
2012/0143650 A1 6/2012 Crowley et al.
2012/0144499 A1 6/2012 Tan et al.
2012/0191596 A1 7/2012 Kremen et al.
2012/0226621 A1 9/2012 Petran et al.
2012/0239557 A1 9/2012 Weinflash et al.
2012/0254320 A1 10/2012 Dove et al.
2012/0259752 A1 10/2012 Agee
2012/0323700 A1 12/2012 Aleksandrovich et al.
2012/0330769 A1 12/2012 Arceo
2012/0330869 A1 12/2012 Durham
2013/0004933 A1 1/2013 Bhaskaran
2013/0018954 A1 1/2013 Cheng
2013/0085801 A1 4/2013 Sharpe et al.
2013/0091156 A1 4/2013 Raiche et al.
2013/0103485 A1 4/2013 Postrel
2013/0111323 A1 5/2013 Taghaddos et al.
2013/0124257 A1 5/2013 Schubert
2013/0159351 A1 6/2013 Hamann et al.
2013/0160120 A1 6/2013 Malaviya et al.
2013/0171968 A1 7/2013 Wang
2013/0179982 A1 7/2013 Bridges et al.
2013/0179988 A1 7/2013 Bekker et al.
2013/0185806 A1 7/2013 Hatakeyama
2013/0211872 A1 8/2013 Cherry et al.
2013/0218829 A1 8/2013 Martinez
2013/0219459 A1 8/2013 Bradley
2013/0254139 A1 9/2013 Lei
2013/0254649 A1 9/2013 Oneill
2013/0254699 A1 9/2013 Bashir et al.
2013/0262328 A1 10/2013 Federgreen
2013/0282438 A1 10/2013 Hunter et al.
2013/0282466 A1 10/2013 Hampton
2013/0290169 A1 10/2013 Bathula et al.
2013/0298071 A1 11/2013 Wine
2013/0311224 A1 11/2013 Heroux et al.
2013/0318207 A1 11/2013 Dotter
2013/0326112 A1 12/2013 Park et al.
2013/0332362 A1 12/2013 Ciurea
2013/0340086 A1 12/2013 Blom
2014/0006355 A1 1/2014 Kirihata
2014/0006616 A1 1/2014 Aad et al.
2014/0012833 A1 1/2014 Humprecht
2014/0019561 A1 1/2014 Belity et al.
2014/0032259 A1 1/2014 Lafever et al.
2014/0032265 A1 1/2014 Paprocki
2014/0040134 A1 2/2014 Ciurea
2014/0040161 A1 2/2014 Berlin
2014/0040979 A1 2/2014 Barton et al.
2014/0041048 A1 2/2014 Goodwin et al.
2014/0047551 A1 2/2014 Nagasundaram et al.
2014/0052463 A1 2/2014 Cashman et al.
2014/0067973 A1 3/2014 Eden
2014/0074550 A1 3/2014 Chourey
2014/0074645 A1 3/2014 Ingram
2014/0075493 A1 3/2014 Krishnan et al.
2014/0089027 A1 3/2014 Brown
2014/0089039 A1 3/2014 McClellan
2014/0108173 A1 4/2014 Cooper et al.
2014/0108968 A1 4/2014 Vishria
2014/0137257 A1 5/2014 Martinez et al.
2014/0142988 A1 5/2014 Grosso et al.
2014/0143011 A1 5/2014 Mudugu et al.
2014/0143844 A1 5/2014 Goertzen
2014/0164476 A1 6/2014 Thomson
2014/0188956 A1 7/2014 Subba et al.
2014/0196143 A1 7/2014 Fliderman et al.
2014/0208418 A1 7/2014 Libin
2014/0222468 A1 8/2014 Araya et al.
2014/0244309 A1 8/2014 Francois
2014/0244325 A1 8/2014 Cartwright
2014/0244375 A1 8/2014 Kim
2014/0244399 A1 8/2014 Orduna et al.
2014/0257917 A1 9/2014 Spencer et al.
2014/0258093 A1 9/2014 Gardiner et al.
2014/0278539 A1 9/2014 Edwards
2014/0278663 A1 9/2014 Samuel et al.
2014/0278730 A1 9/2014 Muhart et al.
2014/0278802 A1 9/2014 MacPherson
2014/0283027 A1 9/2014 Orona et al.
2014/0283106 A1 9/2014 Stahura et al.
2014/0288971 A1 9/2014 Whibbs, III
2014/0289366 A1 9/2014 Choi et al.
2014/0289681 A1 9/2014 Wielgosz
2014/0289862 A1 9/2014 Gorfein et al.
2014/0317171 A1 10/2014 Fox et al.
2014/0324480 A1 10/2014 Dufel et al.
2014/0337041 A1 11/2014 Madden et al.
2014/0337466 A1 11/2014 Li et al.
2014/0344015 A1 11/2014 Puértolas-Montañés et al.
2015/0006514 A1 1/2015 Hung
2015/0012363 A1 1/2015 Grant et al.
2015/0019530 A1 1/2015 Felch
2015/0026056 A1 1/2015 Calman et al.
2015/0026260 A1 1/2015 Worthley
2015/0033112 A1 1/2015 Norwood et al.
2015/0066577 A1 3/2015 Christiansen et al.
2015/0066865 A1 3/2015 Yara et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2015/0074765 A1 3/2015 Haight et al.
2015/0088598 A1 3/2015 Acharyya et al.
2015/0088635 A1 3/2015 Maycotte et al.
2015/0106264 A1 4/2015 Johnson
2015/0106867 A1 4/2015 Liang
2015/0106948 A1 4/2015 Holman et al.
2015/0106949 A1 4/2015 Holman et al.
2015/0121462 A1 4/2015 Courage et al.
2015/0143258 A1 5/2015 Carolan et al.
2015/0149362 A1 5/2015 Baum et al.
2015/0154520 A1 6/2015 Federgreen et al.
2015/0169318 A1 6/2015 Nash
2015/0172296 A1 6/2015 Fujioka
2015/0178740 A1 6/2015 Borawski et al.
2015/0199534 A1 7/2015 Francis et al.
2015/0199541 A1 7/2015 Koch et al.
2015/0199702 A1 7/2015 Singh
2015/0229664 A1 8/2015 Hawthorn et al.
2015/0235049 A1 8/2015 Cohen et al.
2015/0235050 A1 8/2015 Wouhaybi et al.
2015/0235283 A1 8/2015 Nishikawa
2015/0242638 A1 8/2015 Bitran et al.
2015/0242778 A1 8/2015 Wilcox et al.
2015/0242858 A1 8/2015 Smith et al.
2015/0248391 A1 9/2015 Watanabe
2015/0254597 A1 9/2015 Jahagirdar
2015/0261887 A1 9/2015 Joukov
2015/0262189 A1 9/2015 Vergeer
2015/0264417 A1 9/2015 Spitz et al.
2015/0269384 A1 9/2015 Holman et al.
2015/0271167 A1 9/2015 Kalai
2015/0288715 A1 10/2015 Hotchkiss
2015/0309813 A1 10/2015 Patel
2015/0310227 A1 10/2015 Ishida et al.
2015/0310575 A1 10/2015 Shelton
2015/0348200 A1 12/2015 Fair et al.
2015/0356362 A1 12/2015 Demos
2015/0379430 A1 12/2015 Dirac et al.
2016/0006760 A1 1/2016 Lala et al.
2016/0012465 A1 1/2016 Sharp
2016/0026394 A1 1/2016 Goto
2016/0034918 A1 2/2016 Bjelajac et al.
2016/0048700 A1 2/2016 Stransky-Heilkron
2016/0050213 A1 2/2016 Storr
2016/0063523 A1 3/2016 Nistor et al.
2016/0063567 A1 3/2016 Srivastava
2016/0071112 A1 3/2016 Unser
2016/0080405 A1 3/2016 Schler et al.
2016/0099963 A1 4/2016 Mahaffey et al.
2016/0103963 A1 4/2016 Mishra
2016/0125550 A1 5/2016 Joao et al.
2016/0125749 A1 5/2016 Delacroix et al.
2016/0125751 A1 5/2016 Barker et al.
2016/0140466 A1 5/2016 Sidebottom et al.
2016/0143570 A1 5/2016 Valacich et al.
2016/0148143 A1 5/2016 Anderson et al.
2016/0148259 A1 5/2016 Baek et al.
2016/0162269 A1 6/2016 Pogorelik et al.
2016/0164915 A1 6/2016 Cook
2016/0180386 A1 6/2016 Konig
2016/0188450 A1 6/2016 Appusamy et al.
2016/0189156 A1 6/2016 Kim et al.
2016/0196189 A1 7/2016 Miyagi et al.
2016/0225000 A1 8/2016 Glasgow
2016/0232465 A1 8/2016 Kurtz et al.
2016/0232534 A1 8/2016 Lacey et al.
2016/0234319 A1 8/2016 Griffin
2016/0253497 A1 9/2016 Christodorescu et al.
2016/0255139 A1 9/2016 Rathod
2016/0261631 A1 9/2016 Vissamsetty et al.
2016/0262163 A1 9/2016 Gonzalez Garrido et al.
2016/0292453 A1 10/2016 Patterson et al.
2016/0292621 A1 10/2016 Ciccone et al.
2016/0321582 A1 11/2016 Broudou et al.
2016/0321748 A1 11/2016 Mahatma et al.
2016/0330237 A1 11/2016 Edlabadkar
2016/0335531 A1 11/2016 Mullen et al.
2016/0342811 A1 11/2016 Whitcomb et al.
2016/0359861 A1 12/2016 Manov et al.
2016/0364736 A1 12/2016 Maugans, III
2016/0370954 A1 12/2016 Burningham et al.
2016/0378762 A1 12/2016 Rohter
2016/0381064 A1 12/2016 Chan et al.
2016/0381560 A1 12/2016 Margaliot
2017/0004055 A1 1/2017 Horan et al.
2017/0032395 A1 2/2017 Kaufman et al.
2017/0032408 A1 2/2017 Kumar et al.
2017/0034101 A1 2/2017 Kumar et al.
2017/0041324 A1 2/2017 Ionutescu et al.
2017/0046399 A1 2/2017 Sankaranarasimhan et al.
2017/0046753 A1 2/2017 Deupree, IV
2017/0061501 A1 3/2017 Horwich
2017/0068785 A1 3/2017 Experton et al.
2017/0070495 A1 3/2017 Cherry et al.
2017/0075513 A1 3/2017 Watson et al.
2017/0093917 A1 3/2017 Chandra et al.
2017/0115864 A1 4/2017 Thomas et al.
2017/0124570 A1 5/2017 Nidamanuri et al.
2017/0140174 A1 5/2017 Lacey et al.
2017/0140467 A1 5/2017 Neag et al.
2017/0142158 A1 5/2017 Laoutaris et al.
2017/0142177 A1 5/2017 Hu
2017/0154188 A1 6/2017 Meier et al.
2017/0161520 A1 6/2017 Lockhart, III et al.
2017/0171235 A1 6/2017 Mulchandani et al.
2017/0171325 A1 6/2017 Perez
2017/0177324 A1 6/2017 Frank et al.
2017/0180378 A1 6/2017 Tyler et al.
2017/0180505 A1 6/2017 Shaw et al.
2017/0193017 A1 7/2017 Migliori
2017/0193624 A1 7/2017 Tsai
2017/0201518 A1 7/2017 Holmqvist et al.
2017/0206707 A1 7/2017 Guay et al.
2017/0208084 A1 7/2017 Steelman et al.
2017/0213206 A1 7/2017 Shearer
2017/0220685 A1 8/2017 Yan et al.
2017/0220964 A1 8/2017 Datta Ray
2017/0249394 A1 8/2017 Loeb et al.
2017/0249710 A1 8/2017 Guillama et al.
2017/0269791 A1 9/2017 Meyerzon et al.
2017/0270318 A1 9/2017 Ritchie
2017/0278004 A1 9/2017 McElhinney et al.
2017/0278117 A1 9/2017 Wallace et al.
2017/0286719 A1 10/2017 Krishnamurthy et al.
2017/0287031 A1 10/2017 Barday
2017/0289199 A1 10/2017 Barday
2017/0308875 A1 10/2017 O'Regan et al.
2017/0316400 A1 11/2017 Venkatakrishnan et al.
2017/0330197 A1 11/2017 DiMaggio et al.
2017/0353404 A1 12/2017 Hodge
2018/0032757 A1 2/2018 Michael
2018/0039975 A1 2/2018 Hefetz
2018/0041498 A1 2/2018 Kikuchi
2018/0046753 A1 2/2018 Shelton
2018/0046939 A1 2/2018 Meron et al.
2018/0063174 A1 3/2018 Grill et al.
2018/0063190 A1 3/2018 Wright et al.
2018/0082024 A1 3/2018 Curbera et al.
2018/0082368 A1 3/2018 Weinflash et al.
2018/0083843 A1 3/2018 Sambandam
2018/0091476 A1 3/2018 Jakobsson et al.
2018/0131574 A1 5/2018 Jacobs et al.
2018/0131658 A1 5/2018 Bhagwan et al.
2018/0165637 A1 6/2018 Romero et al.
2018/0198614 A1 7/2018 Neumann
2018/0204281 A1 7/2018 Painter et al.
2018/0219917 A1 8/2018 Chiang
2018/0239500 A1 8/2018 Allen et al.
2018/0248914 A1 8/2018 Sartor
2018/0285887 A1 10/2018 Maung
2018/0301222 A1 10/2018 Dew, Sr. et al.
2018/0307859 A1 10/2018 Lafever et al.
2018/0336509 A1 11/2018 Guttmann
2018/0343215 A1 11/2018 Ganapathi et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2018/0349583 A1 12/2018 Turgeman et al.
2018/0351888 A1 12/2018 Howard
2018/0352003 A1 12/2018 Winn et al.
2018/0357243 A1 12/2018 Yoon
2018/0365720 A1 12/2018 Goldman et al.
2018/0374030 A1 12/2018 Barday et al.
2018/0375814 A1 12/2018 Hart
2019/0005210 A1 1/2019 Wiederspohn et al.
2019/0012211 A1 1/2019 Selvaraj
2019/0012672 A1 1/2019 Francesco
2019/0019184 A1 1/2019 Lacey et al.
2019/0050547 A1 2/2019 Welsh et al.
2019/0087570 A1 3/2019 Sloane
2019/0096020 A1 3/2019 Barday et al.
2019/0108353 A1 4/2019 Sadeh et al.
2019/0130132 A1 5/2019 Barbas et al.
2019/0138496 A1 5/2019 Yamaguchi
2019/0139087 A1 5/2019 Dabbs et al.
2019/0148003 A1 5/2019 Van Hoe
2019/0156053 A1 5/2019 Vogel et al.
2019/0156058 A1 5/2019 Van Dyne et al.
2019/0171801 A1 6/2019 Barday et al.
2019/0179652 A1 6/2019 Hesener et al.
2019/0180051 A1 6/2019 Barday et al.
2019/0182294 A1 6/2019 Rieke et al.
2019/0188402 A1 6/2019 Wang et al.
2019/0266200 A1 8/2019 Francolla
2019/0266201 A1 8/2019 Barday et al.
2019/0266350 A1 8/2019 Barday et al.
2019/0268343 A1 8/2019 Barday et al.
2019/0268344 A1 8/2019 Barday et al.
2019/0272492 A1 9/2019 Elledge et al.
2019/0294818 A1 9/2019 Barday et al.
2019/0332802 A1 10/2019 Barday et al.
2019/0332807 A1 10/2019 Lafever et al.
2019/0333118 A1 10/2019 Crimmins et al.
2019/0354709 A1 11/2019 Brinskelle
2019/0356684 A1 11/2019 Sinha et al.
2019/0362169 A1 11/2019 Lin et al.
2019/0362268 A1 11/2019 Fogarty et al.
2019/0377901 A1 12/2019 Balzer et al.
2019/0378073 A1 12/2019 Lopez et al.
2019/0384934 A1 12/2019 Kim
2019/0392162 A1 12/2019 Stern et al.
2019/0392170 A1 12/2019 Barday et al.
2019/0392171 A1 12/2019 Barday et al.
2020/0020454 A1 1/2020 McGarvey et al.
2020/0050966 A1 2/2020 Enuka et al.
2020/0051117 A1 2/2020 Mitchell
2020/0057781 A1 2/2020 McCormick
2020/0074471 A1 3/2020 Adjaoute
2020/0081865 A1 3/2020 Farrar et al.
2020/0082270 A1 3/2020 Gu et al.
2020/0090197 A1 3/2020 Rodriguez et al.
2020/0092179 A1 3/2020 Chieu et al.
2020/0110589 A1 4/2020 Bequet et al.
2020/0110904 A1 4/2020 Shinde et al.
2020/0117737 A1 4/2020 Gopalakrishnan et al.
2020/0137097 A1 4/2020 Zimmermann et al.
2020/0143301 A1 5/2020 Bowers
2020/0143797 A1 5/2020 Manoharan et al.
2020/0159952 A1 5/2020 Dain et al.
2020/0159955 A1 5/2020 Barlik et al.
2020/0167653 A1 5/2020 Manjunath et al.
2020/0175424 A1 6/2020 Kursun
2020/0183655 A1 6/2020 Barday et al.
2020/0186355 A1 6/2020 Davies
2020/0193018 A1 6/2020 Van Dyke
2020/0193022 A1 6/2020 Lunsford et al.
2020/0210558 A1 7/2020 Barday et al.
2020/0210620 A1 7/2020 Haletky
2020/0211002 A1 7/2020 Steinberg
2020/0220901 A1 7/2020 Barday et al.
2020/0226156 A1 7/2020 Borra et al.
2020/0226196 A1 7/2020 Brannon et al.
2020/0242259 A1 7/2020 Chirravuri et al.
2020/0242719 A1 7/2020 Lee
2020/0250342 A1 8/2020 Miller et al.
2020/0252413 A1 8/2020 Buzbee et al.
2020/0252817 A1 8/2020 Brouillette et al.
2020/0272764 A1 8/2020 Brannon et al.
2020/0285755 A1 9/2020 Kassoumeh et al.
2020/0293679 A1 9/2020 Handy Bosma et al.
2020/0296171 A1 9/2020 Mocanu et al.
2020/0302089 A1 9/2020 Barday et al.
2020/0310917 A1 10/2020 Tkachev et al.
2020/0311310 A1 10/2020 Barday et al.
2020/0344243 A1 10/2020 Brannon et al.
2020/0356695 A1 11/2020 Brannon et al.
2020/0364369 A1 11/2020 Brannon et al.
2020/0372178 A1 11/2020 Barday et al.
2020/0394327 A1 12/2020 Childress et al.
2020/0401380 A1 12/2020 Jacobs et al.
2020/0401962 A1 12/2020 Gottemukkala et al.
2020/0410117 A1 12/2020 Barday et al.
2020/0410131 A1 12/2020 Barday et al.
2020/0410132 A1 12/2020 Brannon et al.
2021/0012341 A1 1/2021 Garg et al.
2021/0056569 A1 2/2021 Silberman et al.
2021/0075775 A1 3/2021 Cheng et al.
2021/0081567 A1 3/2021 Park et al.
2021/0099449 A1 4/2021 Frederick et al.
2021/0110047 A1 4/2021 Fang
2021/0124821 A1 4/2021 Spivak et al.
2021/0125089 A1 4/2021 Nickl et al.
2021/0152496 A1 5/2021 Kim et al.
2021/0182940 A1 6/2021 Gupta et al.
2021/0224402 A1 7/2021 Sher-Jan et al.
2021/0233157 A1 7/2021 Crutchfield, Jr.
2021/0243595 A1 8/2021 Buck et al.
2021/0248247 A1 8/2021 Poothokaran et al.
2021/0256163 A1 8/2021 Fleming et al.
2021/0279360 A1 9/2021 Gimenez Palop et al.
2021/0288995 A1 9/2021 Attar et al.
2021/0297441 A1 9/2021 Olalere
2021/0303828 A1 9/2021 Lafreniere et al.
2021/0312061 A1 10/2021 Schroeder et al.
2021/0314328 A1 10/2021 Simons
2021/0326786 A1 10/2021 Sun et al.
2021/0328969 A1 10/2021 Gaddam et al.
2021/0350022 A1 11/2021 Brannon et al.
2021/0382949 A1 12/2021 Yastrebenetsky et al.
2021/0397735 A1 12/2021 Samatov et al.
2021/0400018 A1 12/2021 Vettaikaran et al.
2021/0406712 A1 12/2021 Bhide et al.
2022/0004663 A1 1/2022 Brannon et al.
2022/0137850 A1 5/2022 Boddu et al.
2022/0171759 A1 6/2022 Jindal et al.
2022/0217045 A1 7/2022 Blau et al.
2022/0414255 A1 12/2022 Wang et al.

FOREIGN PATENT DOCUMENTS

CN	111496802	8/2020
CN	112115859	12/2020
EP	1394698	3/2004
EP	2031540	3/2009
KR	20130024345	3/2013
KR	20130062500	6/2013
WO	2001033430	5/2001
WO	20020067158	8/2002
WO	20030050773	6/2003
WO	2005008411	1/2005
WO	2007002412	1/2007
WO	2008/134203	11/2008
WO	2012174659	12/2012
WO	2015116905	8/2015

(56) **References Cited**

FOREIGN PATENT DOCUMENTS

WO	2020/146028	7/2020
WO	2022006421	1/2022

OTHER PUBLICATIONS

Cruz et al, "Interactive User Feedback in Ontology Matching Using Signature Vectors," IEEE, pp. 1321-1324 (Year: 2012).
Cudre-Mauroux, "ESWC 2008 Ph.D. Symposium," The ESWC 2008 Ph.D. Symposium is sponsored by the Okkam project (http://fp7.okkam.org/), MIT, pp. 1-92 (Year: 2008).
Dowling, "Auditing Global HR Compliance," published May 23, 2014, retrieved from https://www.shrm.org/resourcesandtools/hr-topics/ global-hr/pages/auditing-global-hr-compliance.aspx Jul. 2, 2022 (Year: 2014).
Final Office Action, dated Jul. 1, 2022, from corresponding U.S. Appl. No. 17/187,329.
Final Office Action, dated Jul. 6, 2022, from corresponding U.S. Appl. No. 17/200,698.
Final Office Action, dated Jun. 29, 2022, from corresponding U.S. Appl. No. 17/020,275.
Final Office Action, dated Sep. 19, 2022, from corresponding U.S. Appl. No. 17/306,496.
Heil et al, "Downsizing and Rightsizing, " https://web.archive.org/web/20130523153311/https://www.referenceforbusiness.com/management/De-Ele/Downsizing-and-Rightsizing.html (Year: 2013).
Notice of Allowance, dated Aug. 22, 2022, from corresponding U.S. Appl. No. 17/499,595.
Notice of Allowance, dated Aug. 3, 2022, from corresponding U.S. Appl. No. 17/668,714.
Notice of Allowance, dated Aug. 4, 2022, from corresponding U.S. Appl. No. 17/670,349.
Notice of Allowance, dated Aug. 9, 2022, from corresponding U.S. Appl. No. 17/832,313.
Notice of Allowance, dated Jul. 20, 2022, from corresponding U.S. Appl. No. 16/938,509.
Notice of Allowance, dated Jul. 27, 2022, from corresponding U.S. Appl. No. 17/679,750.
Notice of Allowance, dated Jul. 29, 2022, from corresponding U.S. Appl. No. 17/670,341.
Notice of Allowance, dated Jul. 7, 2022, from corresponding U.S. Appl. No. 17/571,871.
Notice of Allowance, dated Jun. 29, 2022, from corresponding U.S. Appl. No. 17/675,118.
Notice of Allowance, dated Sep. 1, 2022, from corresponding U.S. Appl. No. 17/480,377.
Notice of Allowance, dated Sep. 12, 2022, from corresponding U.S. Appl. No. 17/674,187.
Notice of Allowance, dated Sep. 2, 2022, from corresponding U.S. Appl. No. 17/380,485.
Notice of Allowance, dated Sep. 28, 2022, from corresponding U.S. Appl. No. 17/509,974.
Notice of Allowance, dated Sep. 28, 2022, from corresponding U.S. Appl. No. 17/689,683.
Office Action, dated Aug. 12, 2022, from corresponding U.S. Appl. No. 17/679,734.
Office Action, dated Aug. 17, 2022, from corresponding U.S. Appl. No. 17/373,444.
Office Action, dated Aug. 17, 2022, from corresponding U.S. Appl. No. 17/836,430.
Office Action, dated Aug. 19, 2022, from corresponding U.S. Appl. No. 17/584,187.
Office Action, dated Aug. 2, 2022, from corresponding U.S. Appl. No. 17/670,354.
Office Action, dated Aug. 4, 2022, from corresponding U.S. Appl. No. 17/828,953.
Office Action, dated Jul. 27, 2022, from corresponding U.S. Appl. No. 17/831,713.
Office Action, dated Jul. 28, 2022, from corresponding U.S. Appl. No. 16/925,550.
Office Action, dated Jul. 7, 2022, from corresponding U.S. Appl. No. 17/370,650.
Office Action, dated Sep. 16, 2022, from corresponding U.S. Appl. No. 17/306,438.
Office Action, dated Sep. 2, 2022, from corresponding U.S. Appl. No. 17/499,624.
Office Action, dated Sep. 8, 2022, from corresponding U.S. Appl. No. 17/850,244.
Choi et al, "A Survey on Ontology Mapping," ACM, pp. 34-41 (Year: 2006).
Cui et al, "Domain Ontology Management Environment," IEEE, pp. 1-9 (Year: 2000).
Falbo et al, "An Ontological Approach to Domain Engineering," ACM, pp. 351-358 (Year: 2002).
Final Office Action, dated Jun. 10, 2022, from corresponding U.S. Appl. No. 17/161,159.
Final Office Action, dated Jun. 9, 2022, from corresponding U.S. Appl. No. 17/494,220.
International Search Report, dated Jun. 22, 2022, from corresponding International Application No. PCT/US2022/019358.
International Search Report, dated Jun. 24, 2022, from corresponding International Application No. PCT/US2022/019882.
Notice of Allowance, dated Jun. 14, 2022, from corresponding U.S. Appl. No. 17/679,734.
Notice of Allowance, dated Jun. 16, 2022, from corresponding U.S. Appl. No. 17/119,080.
Notice of Allowance, dated Jun. 23, 2022, from corresponding U.S. Appl. No. 17/588,645.
Notice of Allowance, dated Jun. 8, 2022, from corresponding U.S. Appl. No. 17/722,551.
Office Action, dated Jun. 14, 2022, from corresponding U.S. Appl. No. 17/346,586.
Office Action, dated Jun. 16, 2022, from corresponding U.S. Appl. No. 17/689,683.
Ozdikis et al, "Tool Support for Transformation from an OWL Ontology to an HLA Object Model," ACM, pp. 1-6 (Year: 2010).
Wong et al, "Ontology Mapping for the Interoperability Problem in Network Management," IEEE, pp. 2058-2068 (Year: 2005).
Written Opinion of the International Searching Authority, dated Jun. 22, 2022, from corresponding International Application No. PCT/US2022/019358.
Written Opinion of the International Searching Authority, dated Jun. 24, 2022, from corresponding International Application No. PCT/US2022/019882.
Choe et al, "Understanding Quantified-Selfers' Practices in Collecting and Exploring Personal Data," ACM, pp. 1143-1152 (Year: 2014).
Final Office Action, dated Feb. 8, 2024, from corresponding U.S. Appl. No. 17/743,749.
Final Office Action, dated Jan. 4, 2024, from corresponding U.S. Appl. No. 18/116,791.
Jesus et al, "Consent Receipts for a Usable and Auditable Web of Personal Data," IEEE, pp. 28545-28563 (Year: 2022).
Notice of Allowance, dated Nov. 16, 2023, from corresponding U.S. Appl. No. 17/942,242.
Notice of Allowance, dated Nov. 30, 2023, from corresponding U.S. Appl. No. 18/104,981.
Office Action, dated Feb. 14, 2024, from corresponding U.S. Appl. No. 17/717,587.
Office Action, dated Jan. 16, 2024, from corresponding U.S. Appl. No. 18/110,511.
Su et al, "Privacy as a Service: Protecting the Individual in Healthcare Data Processing," IEEE, pp. 49-59 (Year: 2016).
Notice of Allowance, dated Nov. 16, 2022, from corresponding U.S. Appl. No. 17/860,255.
Notice of Allowance, dated Nov. 9, 2022, from corresponding U.S. Appl. No. 17/187,329.
Notice of Allowance, dated Sep. 30, 2022, from corresponding U.S. Appl. No. 17/867,068.
Office Action, dated Nov. 15, 2022, from corresponding U.S. Appl. No. 17/200,698.

(56) **References Cited**

OTHER PUBLICATIONS

Office Action, dated Oct. 27, 2022, from corresponding U.S. Appl. No. 17/161,159.
Beelders et al, "The Influence of Syntax Highlighting on Scanning and Reading Behaviour for Source Code," SAICSIT Sep. 26-28, 2016, Johannesburg, South Africa, ACM, pp. 1-10 (Year: 2016).
Final Office Action, dated Aug. 17, 2023, from corresponding U.S. Appl. No. 17/872,266.
Hall-Holt et al, "Stripe Boundary Codes for Real-Time Structured-Light Range Scanning of Moving Objects," IEEE, pp. 359-366 (Year: 2001).
International Search Report, dated Aug. 9, 2023, from corresponding International Application No. PCT/US2023/011446.
Office Action, dated Aug. 17, 2023, from corresponding U.S. Appl. No. 17/942,242.
Office Action, dated Aug. 9, 2023, from corresponding U.S. Appl. No. 17/743,749.
Office Action, dated Sep. 21, 2023, from corresponding U.S. Appl. No. 18/116,791.
Written Opinion of the International Searching Authority, dated Aug. 9, 2023, from corresponding International Application No. PCT/US2023/011446.
Final Office Action, dated Mar. 13, 2023, from corresponding U.S. Appl. No. 17/161,159.
International Search Report, dated Jan. 27, 2023, from corresponding International Application No. PCT/US2022/045520.
Notice of Allowance, dated Feb. 14, 2023, from corresponding U.S. Appl. No. 17/373,444.
Notice of Allowance, dated Feb. 2, 2023, from corresponding U.S. Appl. No. 17/850,244.
Notice of Allowance, dated Jan. 25, 2023, from corresponding U.S. Appl. No. 17/675,760.
Notice of Allowance, dated Mar. 13, 2023, from corresponding U.S. Appl. No. 17/200,698.
Office Action, dated Feb. 2, 2023, from corresponding U.S. Appl. No. 17/872,266.
Office Action, dated Jan. 12, 2023, from corresponding U.S. Appl. No. 17/872,084.
Written Opinion of the International Searching Authority, dated Jan. 27, 2023, from corresponding International Application No. PCT/US2022/045520.
Hammer, Eran et al., "The OAuth 2.0 Authorization Framework; draft-ietf-oauth-v2-26," Internet Engineering Task Force, IETF; StandardWorkingDraft, Internet Society (ISOC) 4, Rue Des Falaises CH-1205 Geneva, Switzerland, Jun. 8, 2012 (Jun. 8, 2012), pp. 1-71, XP015083227, [retrieved on Jun. 8, 2012] the whole document.
Invitation to Pay Additional Fees, dated May 2, 2023, from corresponding International Application No. PCT/US2023/011446.
Notice of Allowance, dated Jul. 26, 2023, from corresponding U.S. Appl. No. 18/109,556.
Notice of Allowance, dated Jun. 2, 2023, from corresponding U.S. Appl. No. 18/096,935.
Notice of Allowance, dated May 10, 2023, from corresponding U.S. Appl. No. 17/872,084.
Office Action, dated Jul. 20, 2023, from corresponding U.S. Appl. No. 18/104,981.
Office Action, dated May 4, 2023, from corresponding U.S. Appl. No. 18/096,935.
International Search Report, dated Mar. 4, 2019, from corresponding International Application No. PCT/US2018/055774.
International Search Report, dated Nov. 12, 2021, from corresponding International Application No. PCT/US2021/043481.
International Search Report, dated Nov. 19, 2018, from corresponding International Application No. PCT/US2018/046939.
International Search Report, dated Nov. 3, 2021, from corresponding International Application No. PCT/US2021/040893.
International Search Report, dated Nov. 3, 2021, from corresponding International Application No. PCT/US2021/044910.
International Search Report, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043975.
International Search Report, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043976.
International Search Report, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043977.
International Search Report, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/044026.
International Search Report, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/045240.
International Search Report, dated Oct. 12, 2017, from corresponding International Application No. PCT/US2017/036888.
International Search Report, dated Oct. 12, 2018, from corresponding International Application No. PCT/US2018/044046.
International Search Report, dated Oct. 16, 2018, from corresponding International Application No. PCT/US2018/045243.
International Search Report, dated Oct. 18, 2018, from corresponding International Application No. PCT/US2018/045249.
International Search Report, dated Oct. 20, 2017, from corresponding International Application No. PCT/US2017/036917.
Intemational Search Report, dated Oct. 3, 2017, from corresponding International Application No. PCT/US2017/036912.
International Search Report, dated Sep. 1, 2017, from corresponding International Application No. PCT/US2017/036896.
International Search Report, dated Sep. 12, 2018, from corresponding International Application No. PCT/US2018/037504.
International Search Report, dated Sep. 15, 2021, from corresponding International Application No. PCT/US2021/033631.
Invitation to Pay Additional Search Fees, dated Aug. 10, 2017, from corresponding International Application No. PCT/US2017/036912.
Invitation to Pay Additional Search Fees, dated Aug. 10, 2017, from corresponding International Application No. PCT/US2017/036917.
Invitation to Pay Additional Search Fees, dated Aug. 24, 2017, from corresponding International Application No. PCT/US2017/036888.
Invitation to Pay Additional Search Fees, dated Jan. 18, 2019, from corresponding International Application No. PCT/US2018/055736.
Invitation to Pay Additional Search Fees, dated Jan. 7, 2019, from corresponding International Application No. PCT/US2018/055773.
Invitation to Pay Additional Search Fees, dated Jan. 8, 2019, from corresponding International Application No. PCT/US2018/055774.
Invitation to Pay Additional Search Fees, dated Oct. 23, 2018, from corresponding International Application No. PCT/US2018/045296.
Lebeau, Franck, et al, "Model-Based Vulnerability Testing for Web Applications," 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops, pp. 445-452, IEEE, 2013 (Year: 2013).
Liu, Yandong, et al, "Finding the Right Consumer: Optimizing for Conversion in Display Advertising Campaigns," Proceedings of the Fifth ACM International Conference on Web Search and Data Mining, Feb. 2, 2012, pp. 473-428 (Year: 2012).
Lizar et al, "Usable Consents: Tracking and Managing Use of Personal Data with a Consent Transaction Receipt," Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, 2014, pp. 647-652 (Year: 2014).
Ma Ziang, et al, "LibRadar: Fast and Accurate Detection of Third-Party Libraries in Android Apps," 2016 IEEE/ACM 38th IEEE International Conference on Software Engineering Companion (ICSE-C), ACM, May 14, 2016, pp. 653-656, DOI: http://dx.doi.org/10.1145/2889160.2889178, p. 653, r.col, par. 1-3; figure 3 (Year: 2016).
Mandal, et al, "Automated Age Prediction Using Wrinkles Features of Facial Images and Neural Network," International Journal of Emerging Engineering Research and Technology, vol. 5, Issue 2, Feb. 2017, pp. 12-20 (Year: 2017).
Moiso et al, "Towards a User-Centric Personal Data Ecosystem the Role of the Bank of Individual's Data," 2012 16th International Conference on Intelligence in Next Generation Networks, Berlin, 2012, pp. 202-209 (Year: 2012).
Pfeifle, Sam, The Privacy Advisor, IAPP and AvePoint Launch New Free PIA Tool, International Association of Privacy Professionals, Mar. 5, 2014.
Pfeifle, Sam, The Privacy Advisor, IAPP Heads to Singapore with APIA Template in Tow, International Association of Privacy Pro-

(56) **References Cited**

OTHER PUBLICATIONS

fessionals, https://iapp.org/news/a/iapp-heads-to-singapore-with-apia-template_in_tow/, Mar. 28, 2014, p. 1-3.

Qing-Jiang et al, "The (P, a, K) Anonymity Model for Privacy Protection of Personal Information in the Social Networks," 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, vol. 2 IEEE, 2011, pp. 420-423 (Year: 2011).

Srivastava, Agrima, et al, Measuring Privacy Leaks in Online Social Networks, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013.

Tanwar, et al, "Live Forensics Analysis: Violations of Business Security Policy," 2014 International Conference on Contemporary Computing and Informatics (IC31), 2014, pp. 971-976 (Year: 2014).

Thuraisingham, "Security Issues for the Semantic Web," Proceedings 27th Annual International Computer Software and Applications Conference, COMPSAC 2003, Dallas, TX, USA, 2003, pp. 633-638 (Year: 2003).

Written Opinion of the International Searching Authority, dated Jun. 6, 2017, from corresponding International Application No. PCT/US2017/025611.

Written Opinion of the International Searching Authority, dated Apr. 12, 2022, from corresponding International Application No. PCT/US2022/016735.

Written Opinion of the International Searching Authority, dated Aug. 15, 2017, from corresponding International Application No. PCT/US2017/036919.

Written Opinion of the International Searching Authority, dated Aug. 21, 2017, from corresponding International Application No. PCT/US2017/036914.

Written Opinion of the International Searching Authority, dated Aug. 29, 2017, from corresponding International Application No. PCT/US2017/036898.

Written Opinion of the International Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036889.

Written Opinion of the International Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036890.

Written Opinion of the International Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036893.

Written Opinion of the International Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036901.

Written Opinion of the International Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036913.

Written Opinion of the Intemational Searching Authority, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036920.

Written Opinion of the International Searching Authority, dated Dec. 14, 2018, from corresponding International Application No. PCT/US2018/045296.

Golfarelli et al, "Beyond Data Warehousing: What's Next in Business Intelligence?," ACM, pp. 1-6 (Year: 2004).

Gonçalves et al, "The XML Log Standard for Digital Libraries: Analysis, Evolution, and Deployment," IEEE, pp. 312-314 (Year: 2003).

Goni, Kyriaki, "Deletion Process_Only you can see my history: Investigating Digital Privacy, Digital Oblivion, and Control on Personal Data Through an Interactive Art Installation," ACM, 2016, retrieved online on Oct. 3, 2019, pp. 324-333. Retrieved from the Internet URL: http://delivery.acm.org/10.1145/2920000/291.

Gowadia et al, "RDF Metadata for XML Access Control," ACM, pp. 31-48 (Year: 2003).

Grolinger, et al, "Data Management in Cloud Environments: NoSQL and NewSQL Data Stores," Journal of Cloud Computing: Advances, Systems and Applications, pp. 1-24 (Year: 2013).

Guo, et al, "OPAL: A Passe-partout for Web Forms," ACM, pp. 353-356 (Year: 2012).

Gustarini, et al, "Evaluation of Challenges in Human Subject Studies "In-the-Wild" Using Subjects' Personal Smartphones," ACM, pp. 1447-1456 (Year: 2013).

Hacigümüs, Hakan, et al, Executing SQL over Encrypted Data in the Database-Service-Provider Model, ACM, Jun. 4, 2002, pp. 216-227.

Han et al, "Demographic Estimation from Face Images: Human vs. Machine Performance," IEEE, 2015, pp. 1148-1161 (Year: 2015).

Hauch, et al, "Information Intelligence: Metadata for Information Discovery, Access, and Integration," ACM, pp. 793-798 (Year: 2005).

He et al, "A Crowdsourcing Framework for Detecting of Cross-Browser Issues in Web Application," ACM, pp. 1-4, Nov. 6, 2015 (Year: 2015).

Hernandez, et al, "Data Exchange with Data-Metadata Translations," ACM, pp. 260-273 (Year: 2008).

Hinde, "A Model to Assess Organisational Information Privacy Maturity Against the Protection of Personal Information Act" Dissertation University of Cape Town 2014, pp. 1-121 (Year: 2014).

Hodge, et al, "Managing Virtual Data Marts with Metapointer Tables," pp. 1-7 (Year: 2002).

Horrall et al, "Evaluating Risk: IBM's Country Financial Risk and Treasury Risk Scorecards," Jul. 21, 2014, IBM, vol. 58, issue 4, pp. 2:1-2:9 (Year: 2014).

Hu, et al, "Attribute Considerations for Access Control Systems," NIST Special Publication 800-205, Jun. 2019, pp. 1-42 (Year: 2019).

Hu, et al, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)," NIST Special Publication 800-162, pp. 1-54 (Year: 2013).

Huang, et al, "A Study on Information Security Management with Personal Data Protection," IEEE, Dec. 9, 2011, pp. 624-630 (Year: 2011).

Huettner, "Digital Risk Management: Protecting Your Privacy, Improving Security, and Preparing for Emergencies," IEEE, pp. 136-138 (Year: 2006).

Huner et al, "Towards a Maturity Model for Corporate Data Quality Management", ACM, pp. 231-238, 2009 (Year: 2009).

Hunton & Williams LLP, The Role of Risk Management in Data Protection, Privacy Risk Framework and the Risk-based Approach to Privacy, Centre for Information Policy Leadership, Workshop II, Nov. 23, 2014.

Huo et al, "A Cloud Storage Architecture Model for Data-Intensive Applications," IEEE, pp. 1-4 (Year: 2011).

Imran et al, "Searching in Cloud Object Storage by Using a Metadata Model", IEEE, 2014, retrieved online on Apr. 1, 2020, pp. 121-128. Retrieved from the Internet: URL: https://ieeexplore.ieee.org/stamp/stamp.jsp? (Year: 2014).

Iordanou et al, "Tracing Cross Border Web Tracking," Oct. 31, 2018, pp. 329-342, ACM (Year: 2018).

Islam, et al, "Mixture Model Based Label Association Techniques for Web Accessibility," ACM, pp. 67-76 (Year: 2010).

Jayasinghe et al, "Matching Facial Images Using Age Related Morphing Changes," ISSRI, 2009, pp. 2901-2907 (Year: 2009).

Jensen, et al, "Temporal Data Management," IEEE Transactions on Knowledge and Data Engineering, vol. 11, No. 1, Jan./Feb. 1999, pp. 36-44 (Year: 1999).

Jiahao Chen et al. "Fairness Under Unawareness: Assessing Disparity when Protected Class is Unobserved," arxiv.org, Cornell University Library, 201 Olin Library Cornell University, Ithaca, NY 14853, Nov. 27, 2018 (Nov. 27, 2018), Section 2, Figure 2. (Year 2018).

Joel Reardon et al., Secure Data Deletion from Persistent Media, ACM, Nov. 4, 2013, retrieved online on Jun. 13, 2019, pp. 271-283. Retrieved from the Internet: URL: http://delivery.acm.org/10.1145/2520000/2516699/p271-reardon.pdf? (Year: 2013).

Jones et al, "AI and the Ethics of Automating Consent," IEEE, pp. 64-72, May 2018 (Year: 2018).

Joonbakhsh et al, "Mining and Extraction of Personal Software Process measures through IDE Interaction logs," ACM/IEEE, 2018, retrieved online on Dec. 2, 2019, pp. 78-81. Retrieved from the

(56) **References Cited**

OTHER PUBLICATIONS

Internet: URL: http://delivery.acm.org/10.1145/3200000/3196462/p78-joonbakhsh.pdf? (Year: 2018).
Jun et al, "Scalable Multi-Access Flash Store for Big Data Analytics," ACM, pp. 55-64 (Year: 2014).
Khan et al, "Wrinkles Energy Based Age Estimation Using Discrete Cosine Transform," IEEE, 2015, pp. 1-4 (Year: 2015).
Kirkham, et al, "A Personal Data Store for an Internet of Subjects," IEEE, pp. 92-97 (Year: 2011).
Korba, Larry et al.; "Private Data Discovery for Privacy Compliance in Collaborative Environments"; Cooperative Design, Visualization, and Engineering; Springer Berlin Heidelberg; Sep. 21, 2008; pp. 142-150.
Kristian et al, "Human Facial Age Classification Using Active Shape Module, Geometrical Feature, and Support Vendor Machine on Early Growth Stage," ISICO, 2015, pp. 1-8 (Year: 2015).
Krol, Kat, et al, Control versus Effort in Privacy Warnings for Webforms, ACM, Oct. 24, 2016, pp. 13-23.
Lamb et al, "Role-Based Access Control for Data Service Integration", ACM, pp. 3-11 (Year: 2006).
Leadbetter, et al, "Where Big Data Meets Linked Data: Applying Standard Data Models to Environmental Data Streams," IEEE, pp. 2929-2937 (Year: 2016).
Lewis, James et al, "Microservices," Mar. 25, 2014 (Mar. 25, 2014), XP055907494, Retrieved from the Internet: https://martinfowler.com/articles/microservices.html. [retrieved on Mar. 31, 2022].
Li, Ninghui, et al, t-Closeness: Privacy Beyond k-Anonymity and I-Diversity, IEEE, 2014, p. 106-115.
Liu et al, "A Novel Approach for Detecting Browser-based Silent Miner," IEEE, pp. 490-497 (Year: 2018).
Liu et al, "Cross-Geography Scientific Data Transferring Trends and Behavior," ACM, pp. 267-278 (Year: 2018).
Liu et al, "Overview on Ontology Mapping and Approach," IEEE, pp. 592-595 (Year: 2011).
Liu, Kun, et al, A Framework for Computing the Privacy Scores of Users in Online Social Networks, ACM Transactions on Knowledge Discovery from Data, vol. 5, No. 1, Article 6, Dec. 2010, 30 pages.
Lu et al, "An HTTP Flooding Detection Method Based on Browser Behavior," IEEE, pp. 1151-1154 (Year: 2006).
Lu, "How Machine Learning Mitigates Racial Bias in the US Housing Market," Available as SSRN 3489519, pp. 1-73, Nov. 2019 (Year: 2019).
Luu, et al, "Combined Local and Holistic Facial Features for Age-Determination," 2010 11th Int. Conf. Control, Automation, Robotics and Vision, Singapore, Dec. 7, 2010, IEEE, pp. 900-904 (Year: 2010).
Maret et al, "Multimedia Information Interchange: Web Forms Meet Data Servers", IEEE, pp. 499-505 (Year: 1999).
Martin, et al, "Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use," Communications of the ACM, vol. 46, No. 12, Dec. 2003, pp. 258-264. Internet source https://doi.org/10.1145/953460.953509. (Year: 2003).
Sukumar et al, "Review on Modern Data Preprocessing Techniques in Web Usage Mining (WUM)," IEEE, 2016, pp. 64-69 (Year: 2016).
Symantec, Symantex Data Loss Prevention—Discover, monitor, and protect confidential data; 2008; Symantec Corporation; http://www.mssuk.com/images/Symantec%2014552315_IRC_BR_DLP_03.09_sngl.pdf.
Tanasa et al, "Advanced Data Preprocessing for Intersites Web Usage Mining," IEEE, Mar. 2004, pp. 59-65 (Year: 2004).
The Cookie Collective, Optanon Cookie Policy Generator, The Cookie Collective, Year 2016, http://web.archive.org/web/20160324062743/https:/optanon.com/.
TRUSTe Announces General Availability of Assessment Manager for Enterprises to Streamline Data Privacy Management with Automation, PRNewswire, Mar. 4, 2015.
Tsai et al, "Determinants of Intangible Assets Value: The Data Mining Approach," Knowledge Based System, pp. 67-77 http://www.elsevier.com/locate/knosys (Year: 2012).
Tuomas Aura et al., Scanning Electronic Documents for Personally Identifiable Information, ACM, Oct. 30, 2006, retrieved online on Jun. 13, 2019, pp. 41-49. Retrieved from the Internet: URL: http://delivery.acm.org/10.1145/1180000/1179608/p41-aura.pdf? (Year: 2006).
Van Eijk et al, "The Impact of User Location on Cookie Notices (Inside and Outside of the European Union," IEEE Security & Privacy Workshop on Technology and Consumer Protection (CONPRO '19), Jan. 1, 2019 (Year: 2019).
Wang et al, "Revealing Key Non-Financial Factors for Online Credit-Scoring in E-Financing," 2013, IEEE, pp. 1-6 (Year: 2013).
Wang et al, "Secure and Efficient Access to Outsourced Data," ACM, pp. 55-65 (Year: 2009).
Weaver et al, "Understanding Information Preview in Mobile Email Processing", ACM, pp. 303-312, 2011 (Year: 2011).
Wu et al, "Data Mining with Big Data," IEEE, Jan. 2014, pp. 97-107, vol. 26, No. 1, (Year: 2014).
www.truste.com (1), 200150207, Internet Archive Wayback Machine, www.archive.org,Feb. 7, 2015.
Xu, et al, "GatorShare: A File System Framework for High-Throughput Data Management," ACM, pp. 776-786 (Year: 2010).
Yang et al, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE, pp. 1790-1801 (Year: 2013).
Yang et al, "Mining Web Access Sequence with Improved Apriori Algorithm," IEEE, 2017, pp. 780-784 (Year: 2017).
Ye et al, "An Evolution-Based Cache Scheme for Scalable Mobile Data Access," ACM, pp. 1-7 (Year: 2007).
Yin et al, "Multibank Memory Optimization for Parallel Data Access in Multiple Data Arrays", ACM, pp. 1-8 (Year: 2016).
Yiu et al, "Outsourced Similarity Search on Metric Data Assets", IEEE, pp. 338-352 (Year: 2012).
Yu, "Using Data from Social Media Websites to Inspire the Design of Assistive Technology", ACM, pp. 1-2 (Year: 2016).
Yu, et al, "Performance and Fairness Issues in Big Data Transfers," ACM, pp. 9-11 (Year: 2014).
Yue et al, "An Automatic HTTP Cookie Management System," Computer Networks, Elsevier, Amsterdam, NL, vol. 54, No. 13, Sep. 15, 2010, pp. 2182-2198 (Year: 2010).
Zannone, et al, "Maintaining Privacy on Derived Objects," ACM, pp. 10-19 (Year: 2005).
Zeldovich, Nickolai, et al, Making Information Flow Explicit in HiStar, OSDI '06: 7th USENIX Symposium on Operating Systems Design and Implementation, USENIX Association, p. 263-278.
Zhang et al, "Data Transfer Performance Issues for a Web Services Interface to Synchrotron Experiments", ACM, pp. 59-65 (Year: 2007).
Zhang et al, "Dynamic Topic Modeling for Monitoring Market Competition from Online Text and Image Data", ACM, pp. 1425-1434 (Year: 2015).
Zheng, et al, "Methodologies for Cross-Domain Data Fusion: An Overview," IEEE, pp. 16-34 (Year: 2015).
Zheng, et al, "Toward Assured Data Deletion in Cloud Storage," IEEE, vol. 34, No. 3, pp. 101-107 May/Jun. 2020 (Year: 2020).
Zhu, et al, "Dynamic Data Integration Using Web Services," IEEE, pp. 1-8 (Year: 2004).
Bansal et al, "Integrating Big Data: A Semantic Extract-Transform-Load Framework," IEEE, pp. 42-50 (Year: 2015).
Bao et al, "Performance Modeling and Workflow Scheduling of Microservice-Based Applications in Clouds," IEEE Transactions on Parallel and Distributed Systems, vol. 30, No. 9, Sep. 2019, pp. 2101-2116 (Year: 2019).
Bindschaedler et al, "Privacy Through Fake Yet Semantically Real Traces," arxiv.org, Cornell University Library, 201 Olin Library Cornell University Ithaca, NY 14853, May 27, 2015 (Year: 2015).
Castro et al, "Creating Lightweight Ontologies for Dataset Description," IEEE, pp. 1-4 (Year: 2014).
Final Office Action, dated May 24, 2022, from corresponding U.S. Appl. No. 17/499,582.
International Search Report, dated May 12, 2022, from corresponding International Application No. PCT/US2022/015929.
International Search Report, dated May 17, 2022, from corresponding International Application No. PCT/US2022/015241.

(56) **References Cited**

OTHER PUBLICATIONS

International Search Report, dated May 19, 2022, from corresponding International Application No. PCT/US2022/015637.
Lasierra et al, "Data Management in Home Scenarios Using an Autonomic Ontology-Based Approach," IEEE, pp. 94-99 (Year: 2012).
Lenzerini et al, "Ontology-based Data Management," ACM, pp. 5-6 (Year: 2011).
Niu, et al, "Achieving Data Truthfulness and Privacy Preservation in Data Markets", IEEE Transactions on Knowledge and Data Engineering, IEEE Service Centre, Los Alamitos, CA, US, vol. 31, No. 1, Jan. 1, 2019, pp. 105-119 (Year 2019).
Notice of Allowance, dated May 18, 2022, from corresponding U.S. Appl. No. 17/670,354.
Notice of Allowance, dated May 25, 2022, from corresponding U.S. Appl. No. 16/872,031.
Office Action, dated May 24, 2022, from corresponding U.S. Appl. No. 17/674,187.
Preuveneers et al, "Access Control with Delegated Authorization Policy Evaluation for Data-Driven Microservice Workflows," Future Internet 2017, MDPI, pp. 1-21 (Year: 2017).
Thomas et al, "MooM—A Prototype Framework for Management of Ontology Mappings," IEEE, pp. 548-555 (Year: 2011).
Written Opinion of the International Searching Authority, dated May 12, 2022, from corresponding International Application No. PCT/US2022/015929.
Written Opinion of the International Searching Authority, dated May 17, 2022, from corresponding International Application No. PCT/US2022/015241.
Written Opinion of the International Searching Authority, dated May 19, 2022, from corresponding International Application No. PCT/US2022/015637.
Ex Parte Quayle Action, dated May 10, 2022, from corresponding U.S. Appl. No. 17/668,714.
International Search Report, dated Jun. 1, 2022, from corresponding International Application No. PCT/US2022/016930.
Restriction Requirement, dated Apr. 10, 2019, from corresponding U.S. Appl. No. 16/277,715.
Restriction Requirement, dated Apr. 12, 2022, from corresponding U.S. Appl. No. 17/584,187.
Restriction Requirement, dated Apr. 13, 2020, from corresponding U.S. Appl. No. 16/817,136.
Restriction Requirement, dated Apr. 24, 2019, from corresponding U.S. Appl. No. 16/278,122.
Restriction Requirement, dated Aug. 7, 2019, from corresponding U.S. Appl. No. 16/410,866.
Restriction Requirement, dated Aug. 9, 2019, from corresponding U.S. Appl. No. 16/404,399.
Restriction Requirement, dated Dec. 17, 2021, from corresponding U.S. Appl. No. 17/475,244.
Restriction Requirement, dated Dec. 31, 2018, from corresponding U.S. Appl. No. 15/169,668.
Restriction Requirement, dated Dec. 9, 2019, from corresponding U.S. Appl. No. 16/565,395.
Restriction Requirement, dated Jan. 18, 2017, from corresponding U.S. Appl. No. 15/256,430.
Restriction Requirement, dated Jul. 28, 2017, from corresponding U.S. Appl. No. 15/169,658.
Restriction Requirement, dated Jun. 15, 2021, from corresponding U.S. Appl. No. 17/187,329.
Restriction Requirement, dated Jun. 15, 2021, from corresponding U.S. Appl. No. 17/222,556.
Restriction Requirement, dated Jun. 9, 2021, from corresponding U.S. Appl. No. 17/222,725.
Restriction Requirement, dated May 5, 2020, from corresponding U.S. Appl. No. 16/808,489.
Restriction Requirement, dated Nov. 10, 2021, from corresponding U.S. Appl. No. 17/366,754.
Restriction Requirement, dated Nov. 15, 2019, from corresponding U.S. Appl. No. 16/586,202.
Restriction Requirement, dated Nov. 21, 2016, from corresponding U.S. Appl. No. 15/254,901.
Restriction Requirement, dated Nov. 5, 2019, from corresponding U.S. Appl. No. 16/563,744.
Restriction Requirement, dated Oct. 17, 2018, from corresponding U.S. Appl. No. 16/055,984.
Restriction Requirement, dated Oct. 6, 2021, from corresponding U.S. Appl. No. 17/340,699.
Restriction Requirement, dated Sep. 15, 2020, from corresponding U.S. Appl. No. 16/925,628.
Restriction Requirement, dated Sep. 9, 2019, from corresponding U.S. Appl. No. 16/505,426.
Final Office Action, dated Apr. 1, 2022, from corresponding U.S. Appl. No. 17/370,650.
Final Office Action, dated Apr. 23, 2020, from corresponding U.S. Appl. No. 16/572,347.
Final Office Action, dated Apr. 25, 2022, from corresponding U.S. Appl. No. 17/149,421.
Final Office Action, dated Apr. 27, 2021, from corresponding U.S. Appl. No. 17/068,454.
Final Office Action, dated Apr. 28, 2022, from corresponding U.S. Appl. No. 16/925,550.
Final Office Action, dated Apr. 5, 2022, from corresponding U.S. Appl. No. 17/013,756.
Final Office Action, dated Apr. 7, 2020, from corresponding U.S. Appl. No. 16/595,327.
Final Office Action, dated Aug. 10, 2020, from corresponding U.S. Appl. No. 16/791,589.
Final Office Action, dated Aug. 27, 2021, from corresponding U.S. Appl. No. 17/161,159.
Final Office Action, dated Aug. 28, 2020, from corresponding U.S. Appl. No. 16/410,336.
Final Office Action, dated Aug. 5, 2020, from corresponding U.S. Appl. No. 16/719,071.
Final Office Action, dated Aug. 9, 2021, from corresponding U.S. Appl. No. 17/119,080.
Final Office Action, dated Dec. 10, 2021, from corresponding U.S. Appl. No. 17/187,329.
Final Office Action, dated Dec. 7, 2020, from corresponding U.S. Appl. No. 16/862,956.
Final Office Action, dated Dec. 9, 2019, from corresponding U.S. Appl. No. 16/410,336.
Final Office Action, dated Feb. 19, 2020, from corresponding U.S. Appl. No. 16/404,491.
Final Office Action, dated Feb. 25, 2022, from corresponding U.S. Appl. No. 17/346,586.
Final Office Action, dated Feb. 3, 2020, from corresponding U.S. Appl. No. 16/557,392.
Final Office Action, dated Feb. 8, 2021, from corresponding U.S. Appl. No. 16/927,658.
Final Office Action, dated Jan. 17, 2018, from corresponding U.S. Appl. No. 15/619,278.
Final Office Action, dated Jan. 21, 2020, from corresponding U.S. Appl. No. 16/410,762.
Final Office Action, dated Jan. 23, 2018, from corresponding U.S. Appl. No. 15/619,479.
Final Office Action, dated Jan. 23, 2020, from corresponding U.S. Appl. No. 16/505,430.
Final Office Action, dated Jul. 21, 2021, from corresponding U.S. Appl. No. 17/151,334.
Final Office Action, dated Jul. 7, 2021, from corresponding U.S. Appl. No. 17/149,421.
Final Office Action, dated Mar. 21, 2022, from corresponding U.S. Appl. No. 17/373,444.
Final Office Action, dated Mar. 22, 2022, from corresponding U.S. Appl. No. 17/380,485.
Notice of Allowance, dated Feb. 27, 2019, from corresponding U.S. Appl. No. 16/041,468.
Notice of Allowance, dated Feb. 27, 2019, from corresponding U.S. Appl. No. 16/226,290.
Notice of Allowance, dated Feb. 3, 2021, from corresponding U.S. Appl. No. 16/827,039.

(56) **References Cited**

OTHER PUBLICATIONS

Notice of Allowance, dated Feb. 3, 2021, from corresponding U.S. Appl. No. 17/068,558.
Notice of Allowance, dated Feb. 4, 2022, from corresponding U.S. Appl. No. 17/520,272.
Notice of Allowance, dated Feb. 8, 2022, from corresponding U.S. Appl. No. 17/342,153.
Notice of Allowance, dated Jan. 1, 2021, from corresponding U.S. Appl. No. 17/026,727.
Notice of Allowance, dated Jan. 11, 2022, from corresponding U.S. Appl. No. 17/371,350.
Notice of Allowance, dated Jan. 12, 2022, from corresponding U.S. Appl. No. 17/334,948.
Notice of Allowance, dated Jan. 12, 2022, from corresponding U.S. Appl. No. 17/463,775.
Notice of Allowance, dated Jan. 14, 2020, from corresponding U.S. Appl. No. 16/277,715.
Notice of Allowance, dated Jan. 15, 2021, from corresponding U.S. Appl. No. 17/030,714.
Notice of Allowance, dated Jan. 18, 2018, from corresponding U.S. Appl. No. 15/619,478.
Notice of Allowance, dated Jan. 18, 2019 from corresponding U.S. Appl. No. 16/159,635.
Notice of Allowance, dated Jan. 2, 2020, from corresponding U.S. Appl. No. 16/410,296.
Notice of Allowance, dated Jan. 23, 2018, from corresponding U.S. Appl. No. 15/619,251.
Notice of Allowance, dated Jan. 24, 2022, from corresponding U.S. Appl. No. 17/340,699.
Notice of Allowance, dated Jan. 25, 2021, from corresponding U.S. Appl. No. 16/410,336.
Notice of Allowance, dated Jan. 26, 2018, from corresponding U.S. Appl. No. 15/619,469.
Notice of Allowance, dated Jan. 26, 2022, from corresponding U.S. Appl. No. 17/491,906.
Notice of Allowance, dated Jan. 29, 2020, from corresponding U.S. Appl. No. 16/278,119.
Notice of Allowance, dated Jan. 31, 2022, from corresponding U.S. Appl. No. 17/472,948.
Notice of Allowance, dated Jan. 5, 2022, from corresponding U.S. Appl. No. 17/475,241.
Notice of Allowance, dated Jan. 6, 2021, from corresponding U.S. Appl. No. 16/595,327.
Notice of Allowance, dated Jan. 6, 2022, from corresponding U.S. Appl. No. 17/407,765.
Notice of Allowance, dated Jan. 7, 2022, from corresponding U.S. Appl. No. 17/222,725.
Notice of Allowance, dated Jan. 8, 2020, from corresponding U.S. Appl. No. 16/600,879.
Notice of Allowance, dated Jul. 10, 2019, from corresponding U.S. Appl. No. 16/237,083.
Notice of Allowance, dated Jul. 10, 2019, from corresponding U.S. Appl. No. 16/403,358.
Notice of Allowance, dated Jul. 12, 2019, from corresponding U.S. Appl. No. 16/278,121.
Notice of Allowance, dated Jul. 14, 2020, from corresponding U.S. Appl. No. 16/701,043.
Notice of Allowance, dated Jul. 15, 2020, from corresponding U.S. Appl. No. 16/791,006.
Notice of Allowance, dated Jul. 16, 2020, from corresponding U.S. Appl. No. 16/901,979.
Notice of Allowance, dated Jul. 17, 2019, from corresponding U.S. Appl. No. 16/055,961.
Notice of Allowance, dated Jul. 17, 2020, from corresponding U.S. Appl. No. 16/778,709.
Notice of Allowance, dated Jul. 19, 2021, from corresponding U.S. Appl. No. 17/306,252.
Notice of Allowance, dated Jul. 21, 2020, from corresponding U.S. Appl. No. 16/557,392.
Notice of Allowance, dated Jul. 23, 2019, from corresponding U.S. Appl. No. 16/220,978.
Notice of Allowance, dated Jul. 26, 2019, from corresponding U.S. Appl. No. 16/409,673.
Notice of Allowance, dated Jul. 26, 2021, from corresponding U.S. Appl. No. 17/151,399.
Notice of Allowance, dated Jul. 26, 2021, from corresponding U.S. Appl. No. 17/207,316.
Notice of Allowance, dated Jul. 31, 2019, from corresponding U.S. Appl. No. 16/221,153.
Notice of Allowance, dated Jul. 8, 2021, from corresponding U.S. Appl. No. 17/201,040.
Notice of Allowance, dated Jun. 1, 2020, from corresponding U.S. Appl. No. 16/813,321.
Notice of Allowance, dated Jun. 11, 2021, from corresponding U.S. Appl. No. 16/862,948.
Notice of Allowance, dated Jun. 11, 2021, from corresponding U.S. Appl. No. 16/862,952.
Notice of Allowance, dated Jun. 11, 2021, from corresponding U.S. Appl. No. 17/216,436.
Notice of Allowance, dated Jun. 12, 2019, from corresponding U.S. Appl. No. 16/278,123.
Notice of Allowance, dated Jun. 12, 2019, from corresponding U.S. Appl. No. 16/363,454.
Notice of Allowance, dated Jun. 16, 2020, from corresponding U.S. Appl. No. 16/798,818.
Nemec et al, "Assessment of Query Execution Performance Using Selected Business Intelligence Tools and Experimental Agile Oriented Data Modeling Approach," Sep. 16, 2015, IEEE, pp. 1327-1333. (Year: 2015).
Notice of Allowance, dated Jun. 2, 2022, from corresponding U.S. Appl. No. 17/493,290.
Notice of Allowance, dated May 27, 2022, from corresponding U.S. Appl. No. 17/543,546.
Notice of Allowance, dated May 31, 2022, from corresponding U.S. Appl. No. 17/679,715.
Office Action, dated Jun. 1, 2022, from corresponding U.S. Appl. No. 17/306,496.
Vukovic et al, "Managing Enterprise IT Systems Using Online Communities," Jul. 9, 2011, IEEE, pp. 552-559. (Year: 2011).
Written Opinion of the International Searching Authority, dated Jun. 1, 2022, from corresponding International Application No. PCT/US2022/016930.
Notice of Allowance, dated Jun. 17, 2020, from corresponding U.S. Appl. No. 16/656,895.
Notice of Allowance, dated Jun. 18, 2019, from corresponding U.S. Appl. No. 16/410,566.
Notice of Allowance, dated Jun. 19, 2018, from corresponding U.S. Appl. No. 15/894,890.
Notice of Allowance, dated Jun. 19, 2019, from corresponding U.S. Appl. No. 16/042,673.
Notice of Allowance, dated Jun. 19, 2019, from corresponding U.S. Appl. No. 16/055,984.
Notice of Allowance, dated Jun. 2, 2021, from corresponding U.S. Appl. No. 17/198,581.
Notice of Allowance, dated Jun. 21, 2019, from corresponding U.S. Appl. No. 16/404,439.
Notice of Allowance, dated Jun. 22, 2020, from corresponding U.S. Appl. No. 16/791,337.
Notice of Allowance, dated Jun. 27, 2018, from corresponding U.S. Appl. No. 15/882,989.
Notice of Allowance, dated Jun. 4, 2019, from corresponding U.S. Appl. No. 16/159,566.
Notice of Allowance, dated Jun. 5, 2019, from corresponding U.S. Appl. No. 16/220,899.
Notice of Allowance, dated Jun. 5, 2019, from corresponding U.S. Appl. No. 16/357,260.
Notice of Allowance, dated Jun. 6, 2018, from corresponding U.S. Appl. No. 15/875,570.
Notice of Allowance, dated Jun. 6, 2019, from corresponding U.S. Appl. No. 16/159,628.
Notice of Allowance, dated Jun. 7, 2021, from corresponding U.S. Appl. No. 17/099,270.

(56) **References Cited**

OTHER PUBLICATIONS

Notice of Allowance, dated Jun. 8, 2020, from corresponding U.S. Appl. No. 16/712,104.
Notice of Allowance, dated Mar. 1, 2018, from corresponding U.S. Appl. No. 15/853,674.
Notice of Allowance, dated Mar. 1, 2019, from corresponding U.S. Appl. No. 16/059,911.
Notice of Allowance, dated Mar. 10, 2021, from corresponding U.S. Appl. No. 16/925,628.
Notice of Allowance, dated Mar. 10, 2021, from corresponding U.S. Appl. No. 17/128,666.
Notice of Allowance, dated Mar. 13, 2019, from corresponding U.S. Appl. No. 16/055,083.
Notice of Allowance, dated Mar. 14, 2019, from corresponding U.S. Appl. No. 16/055,944.
Notice of Allowance, dated Mar. 16, 2020, from corresponding U.S. Appl. No. 16/778,704.
Notice of Allowance, dated Mar. 16, 2021, from corresponding U.S. Appl. No. 17/149,380.
Notice of Allowance, dated Mar. 16, 2022, from corresponding U.S. Appl. No. 17/486,350.
Notice of Allowance, dated Mar. 17, 2020, from corresponding U.S. Appl. No. 16/560,885.
Notice of Allowance, dated Mar. 18, 2020, from corresponding U.S. Appl. No. 16/560,963.
Notice of Allowance, dated Mar. 19, 2021, from corresponding U.S. Appl. No. 17/013,757.
Notice of Allowance, dated Mar. 2, 2018, from corresponding U.S. Appl. No. 15/858,802.
Notice of Allowance, dated Mar. 2, 2022, from corresponding U.S. Appl. No. 16/872,130.
Notice of Allowance, dated Mar. 2, 2022, from corresponding U.S. Appl. No. 17/535,098.
Notice of Allowance, dated Mar. 21, 2022, from corresponding U.S. Appl. No. 17/366,754.
Notice of Allowance, dated Mar. 22, 2022, from corresponding U.S. Appl. No. 17/475,244.
Notice of Allowance, dated Mar. 22, 2022, from corresponding U.S. Appl. No. 17/504,102.
Notice of Allowance, dated Mar. 24, 2020, from corresponding U.S. Appl. No. 16/552,758.
Notice of Allowance, dated Mar. 25, 2019, from corresponding U.S. Appl. No. 16/054,780.
Notice of Allowance, dated Mar. 26, 2020, from corresponding U.S. Appl. No. 16/560,889.
Notice of Allowance, dated Mar. 26, 2020, from corresponding U.S. Appl. No. 16/578,712.
Notice of Allowance, dated Mar. 27, 2019, from corresponding U.S. Appl. No. 16/226,280.
Notice of Allowance, dated Mar. 28, 2022, from corresponding U.S. Appl. No. 17/499,609.
Notice of Allowance, dated Mar. 29, 2019, from corresponding U.S. Appl. No. 16/055,998.
Notice of Allowance, dated Mar. 31, 2020, from corresponding U.S. Appl. No. 16/563,744.
Notice of Allowance, dated Mar. 31, 2021, from corresponding U.S. Appl. No. 17/013,758.
Notice of Allowance, dated Mar. 31, 2021, from corresponding U.S. Appl. No. 17/162,205.
Notice of Allowance, dated Mar. 31, 2022, from corresponding U.S. Appl. No. 17/476,209.
Notice of Allowance, dated Mar. 4, 2022, from corresponding U.S. Appl. No. 17/409,999.
Notice of Allowance, dated May 1, 2020, from corresponding U.S. Appl. No. 16/586,202.
Notice of Allowance, dated May 11, 2020, from corresponding U.S. Appl. No. 16/786,196.
Notice of Allowance, dated May 11, 2022, from corresponding U.S. Appl. No. 17/395,759.
Notice of Allowance, dated May 13, 2021, from corresponding U.S. Appl. No. 17/101,915.
Written Opinion of the International Searching Authority, dated Dec. 22, 2021, from corresponding International Application No. PCT/US2021/051217.
Written Opinion of the International Searching Authority, dated Feb. 11, 2022, from corresponding International Application No. PCT/US2021/053518.
Written Opinion of the International Searching Authority, dated Feb. 14, 2022, from corresponding International Application No. PCT/US2021/058274.
Written Opinion of the International Searching Authority, dated Jan. 14, 2019, from corresponding International Application No. PCT/US2018/046949.
Written Opinion of the International Searching Authority, dated Jan. 5, 2022, from corresponding International Application No. PCT/US2021/050497.
Written Opinion of the International Searching Authority, dated Jan. 7, 2019, from corresponding International Application No. PCT/US2018/055772.
Written Opinion of the International Searching Authority, dated Jun. 21, 2017, from corresponding International Application No. PCT/US2017/025600.
Written Opinion of the International Searching Authority, dated Jun. 6, 2017, from corresponding International Application No. PCT/US2017/025605.
Written Opinion of the International Searching Authority, dated Mar. 14, 2019, from corresponding International Application No. PCT/US2018/055736.
Written Opinion of the Intemational Searching Authority, dated Mar. 18, 2022, from corresponding International Application No. PCT/US2022/013733.
Written Opinion of the International Searching Authority, dated Mar. 4, 2019, from corresponding International Application No. PCT/US2018/055773.
Written Opinion of the International Searching Authority, dated Mar. 4, 2019, from corresponding International Application No. PCT/US2018/055774.
Written Opinion of the International Searching Authority, dated Nov. 12, 2021, from corresponding International Application No. PCT/US2021/043481.
Written Opinion of the International Searching Authority, dated Nov. 19, 2018, from corresponding International Application No. PCT/US2018/046939.
Written Opinion of the International Searching Authority, dated Nov. 3, 2021, from corresponding International Application No. PCT/US2021/040893.
Written Opinion of the Intemational Searching Authority, dated Nov. 3, 2021, from corresponding International Application No. PCT/US2021/044910.
Written Opinion of the International Searching Authority, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043975.
Written Opinion of the International Searching Authority, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043976.
Written Opinion of the International Searching Authority, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/043977.
Written Opinion of the International Searching Authority, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/044026.
Written Opinion of the International Searching Authority, dated Oct. 11, 2018, from corresponding International Application No. PCT/US2018/045240.
Written Opinion of the International Searching Authority, dated Oct. 12, 2017, from corresponding International Application No. PCT/US2017/036888.
Written Opinion of the International Searching Authority, dated Oct. 12, 2018, from corresponding International Application No. PCT/US2018/044046.

(56) **References Cited**

OTHER PUBLICATIONS

Written Opinion of the International Searching Authority, dated Oct. 16, 2018, from corresponding International Application No. PCT/US2018/045243.
Written Opinion of the International Searching Authority, dated Oct. 18, 2018, from corresponding International Application No. PCT/US2018/045249.
Written Opinion of the International Searching Authority, dated Oct. 20, 2017, from corresponding International Application No. PCT/US2017/036917.
Written Opinion of the International Searching Authority, dated Oct. 3, 2017, from corresponding International Application No. PCT/US2017/036912.
Written Opinion of the International Searching Authority, dated Sep. 1, 2017, from corresponding International Application No. PCT/US2017/036896.
Written Opinion of the International Searching Authority, dated Sep. 12, 2018, from corresponding International Application No. PCT/US2018/037504.
Written Opinion of the International Searching Authority, dated Sep. 15, 2021, from corresponding International Application No. PCT/US2021/033631.
Abdullah et al, "The Mapping Process of Unstructured Data to the Structured Data", ACM, pp. 151-155 (Year: 2013).
Acar, Gunes, et al, The Web Never Forgets, Computer and Communications Security, ACM, Nov. 3, 2014, pp. 674-689.
Advisory Action, dated Jan. 13, 2021, from corresponding U.S. Appl. No. 16/808,493.
Advisory Action, dated Jan. 13, 2021, from corresponding U.S. Appl. No. 16/862,944.
Advisory Action, dated Jan. 13, 2021, from corresponding U.S. Appl. No. 16/862,948.
Advisory Action, dated Jan. 13, 2021, from corresponding U.S. Appl. No. 16/862,952.
Advisory Action, dated Jan. 6, 2021, from corresponding U.S. Appl. No. 16/808,497.
Advisory Action, dated Jun. 19, 2020, from corresponding U.S. Appl. No. 16/595,342.
Advisory Action, dated Jun. 2, 2020, from corresponding U.S. Appl. No. 16/404,491.
Advisory Action, dated May 21, 2020, from corresponding U.S. Appl. No. 16/557,392.
Aghasian, Erfan, et al, Scoring Users' Privacy Disclosure Across Multiple Online Social Networks,IEEE Access, Multidisciplinary Rapid Review Open Access Journal, Jul. 31, 2017, vol. 5, 2017.
Agosti et al, "Access and Exchange of Hierarchically Structured Resources on the Web with the NESTOR Framework", IEEE, pp. 659-662 (Year: 2009).
Ahmad et al, "Task-Oriented Access Model for Secure Data Sharing Over Cloud," ACM, pp. 1-7 (Year: 2015).
Ahmad, et al, "Performance of Resource Management Algorithms for Processable Bulk Data Transfer Tasks in Grid Environments," ACM, pp. 177-188 (Year: 2008).
Alaa et al, "Personalized Risk Scoring for Critical Care Prognosis Using Mixtures of Gaussian Processes," Apr. 27, 2017, IEEE, vol. 65, issue 1, pp. 207-217 (Year: 2017).
Ali et al, "Age Estimation from Facial Images Using Biometric Ratios and Wrinkle Analysis," IEEE, 2015, pp. 1-5 (Year: 2015).
Aman et al, "Detecting Data Tampering Attacks in Synchrophasor Networks using Time Hopping," IEEE, pp. 1-6 (Year: 2016).
Amar et al, "Privacy-Aware Infrastructure for Managing Personal Data," ACM, pp. 571-572, Aug. 22-26, 2016 (Year: 2016).
Antunes et al, "Preserving Digital Data in Heterogeneous Environments", ACM, pp. 345-348, 2009 (Year: 2009).
Ardagna, et al, "A Privacy-Aware Access Control System," Journal of Computer Security, 16:4, pp. 369-397 (Year: 2008).
Final Office Action, dated Mar. 26, 2021, from corresponding U.S. Appl. No. 17/020,275.
Final Office Action, dated Mar. 5, 2019, from corresponding U.S. Appl. No. 16/055,961.
Final Office Action, dated Mar. 6, 2020, from corresponding U.S. Appl. No. 16/595,342.
Final Office Action, dated May 12, 2022, from corresponding U.S. Appl. No. 17/499,624.
Final Office Action, dated May 14, 2021, from corresponding U.S. Appl. No. 17/013,756.
Final Office Action, dated May 16, 2022, from corresponding U.S. Appl. No. 17/480,377.
Final Office Action, dated May 2, 2022, from corresponding U.S. Appl. No. 17/499,595.
Final Office Action, dated Nov. 29, 2017, from corresponding U.S. Appl. No. 15/619,237.
Final Office Action, dated Oct. 26, 2021, from corresponding U.S. Appl. No. 17/306,496.
Final Office Action, dated Oct. 28, 2021, from corresponding U.S. Appl. No. 17/234,205.
Final Office Action, dated Oct. 29, 2021, from corresponding U.S. Appl. No. 17/020,275.
Final Office Action, dated Sep. 17, 2021, from corresponding U.S. Appl. No. 17/200,698.
Final Office Action, dated Sep. 21, 2020, from corresponding U.S. Appl. No. 16/808,493.
Final Office Action, dated Sep. 21, 2020, from corresponding U.S. Appl. No. 16/862,944.
Final Office Action, dated Sep. 22, 2020, from corresponding U.S. Appl. No. 16/808,497.
Final Office Action, dated Sep. 23, 2020, from corresponding U.S. Appl. No. 16/862,948.
Final Office Action, dated Sep. 24, 2020, from corresponding U.S. Appl. No. 16/862,952.
Final Office Action, dated Sep. 25, 2019, from corresponding U.S. Appl. No. 16/278,119.
Final Office Action, dated Sep. 28, 2020, from corresponding U.S. Appl. No. 16/565,395.
Final Office Action, dated Sep. 8, 2020, from corresponding U.S. Appl. No. 16/410,866.
Office Action, dated Apr. 1, 2021, from corresponding U.S. Appl. No. 17/119,080.
Office Action, dated Apr. 12, 2022, from corresponding U.S. Appl. No. 17/670,341.
Office Action, dated Apr. 15, 2021, from corresponding U.S. Appl. No. 17/161,159.
Office Action, dated Apr. 18, 2018, from corresponding U.S. Appl. No. 15/894,819.
Office Action, dated Apr. 18, 2022, from corresponding U.S. Appl. No. 17/670,349.
Office Action, dated Apr. 2, 2021, from corresponding U.S. Appl. No. 17/151,334.
Office Action, dated Apr. 20, 2020, from corresponding U.S. Appl. No. 16/812,795.
Office Action, dated Apr. 22, 2019, from corresponding U.S. Appl. No. 16/241,710.
Office Action, dated Apr. 22, 2020, from corresponding U.S. Appl. No. 16/811,793.
Office Action, dated Apr. 25, 2022, from corresponding U.S. Appl. No. 17/588,645.
Office Action, dated Apr. 26, 2022, from corresponding U.S. Appl. No. 17/151,334.
Office Action, dated Apr. 28, 2020, from corresponding U.S. Appl. No. 16/798,818.
Office Action, dated Apr. 28, 2020, from corresponding U.S. Appl. No. 16/808,500.
Office Action, dated Apr. 28, 2021, from corresponding U.S. Appl. No. 16/808,497.
Office Action, dated Apr. 29, 2020, from corresponding U.S. Appl. No. 16/791,337.
Office Action, dated Apr. 5, 2019, from corresponding U.S. Appl. No. 16/278,119.
Office Action, dated Apr. 7, 2020, from corresponding U.S. Appl. No. 16/788,633.
Office Action, dated Apr. 7, 2020, from corresponding U.S. Appl. No. 16/791,589.

(56) **References Cited**

OTHER PUBLICATIONS

Office Action, dated Apr. 8, 2022, from corresponding U.S. Appl. No. 16/938,509.
Office Action, dated Aug. 13, 2019, from corresponding U.S. Appl. No. 16/505,430.
Office Action, dated Aug. 13, 2019, from corresponding U.S. Appl. No. 16/512,033.
Office Action, dated Aug. 15, 2019, from corresponding U.S. Appl. No. 16/505,461.
Office Action, dated Aug. 18, 2021, from corresponding U.S. Appl. No. 17/222,725.
Office Action, dated Aug. 19, 2019, from corresponding U.S. Appl. No. 16/278,122.
Office Action, dated Aug. 20, 2020, from corresponding U.S. Appl. No. 16/817,136.
Office Action, dated Aug. 23, 2017, from corresponding U.S. Appl. No. 15/626,052.
Office Action, dated Aug. 24, 2017, from corresponding U.S. Appl. No. 15/169,643.
Office Action, dated Aug. 24, 2017, from corresponding U.S. Appl. No. 15/619,451.
Office Action, dated Aug. 24, 2020, from corresponding U.S. Appl. No. 16/595,327.
Office Action, dated Aug. 27, 2019, from corresponding U.S. Appl. No. 16/410,296.
Notice of Allowance, dated May 19, 2020, from corresponding U.S. Appl. No. 16/505,430.
Notice of Allowance, dated May 19, 2020, from corresponding U.S. Appl. No. 16/808,496.
Notice of Allowance, dated May 20, 2020, from corresponding U.S. Appl. No. 16/707,762.
Notice of Allowance, dated May 21, 2018, from corresponding U.S. Appl. No. 15/896,790.
Notice of Allowance, dated May 26, 2021, from corresponding U.S. Appl. No. 16/808,493.
Notice of Allowance, dated May 26, 2021, from corresponding U.S. Appl. No. 16/865,874.
Notice of Allowance, dated May 26, 2021, from corresponding U.S. Appl. No. 17/199,514.
Notice of Allowance, dated May 27, 2020, from corresponding U.S. Appl. No. 16/820,208.
Notice of Allowance, dated May 27, 2021, from corresponding U.S. Appl. No. 16/927,658.
Notice of Allowance, dated May 27, 2021, from corresponding U.S. Appl. No. 17/198,757.
Notice of Allowance, dated May 28, 2019, from corresponding U.S. Appl. No. 16/277,568.
Notice of Allowance, dated May 28, 2020, from corresponding U.S. Appl. No. 16/799,279.
Notice of Allowance, dated May 28, 2021, from corresponding U.S. Appl. No. 16/862,944.
Notice of Allowance, dated May 5, 2017, from corresponding U.S. Appl. No. 15/254,901.
Notice of Allowance, dated May 5, 2020, from corresponding U.S. Appl. No. 16/563,754.
Notice of Allowance, dated May 6, 2022, from corresponding U.S. Appl. No. 17/666,886.
Notice of Allowance, dated May 7, 2020, from corresponding U.S. Appl. No. 16/505,426.
Notice of Allowance, dated May 7, 2021, from corresponding U.S. Appl. No. 17/194,662.
Notice of Allowance, dated Nov. 14, 2019, from corresponding U.S. Appl. No. 16/436,616.
Notice of Allowance, dated Nov. 16, 2021, from corresponding U.S. Appl. No. 17/491,871.
Notice of Allowance, dated Nov. 2, 2018, from corresponding U.S. Appl. No. 16/054,762.
Notice of Allowance, dated Nov. 22, 2021, from corresponding U.S. Appl. No. 17/383,889.
Notice of Allowance, dated Nov. 23, 2020, from corresponding U.S. Appl. No. 16/791,589.
Notice of Allowance, dated Nov. 24, 2020, from corresponding U.S. Appl. No. 17/027,019.
Notice of Allowance, dated Nov. 25, 2020, from corresponding U.S. Appl. No. 17/019,771.
Notice of Allowance, dated Nov. 26, 2019, from corresponding U.S. Appl. No. 16/563,735.
Notice of Allowance, dated Nov. 27, 2019, from corresponding U.S. Appl. No. 16/570,712.
Notice of Allowance, dated Nov. 27, 2019, from corresponding U.S. Appl. No. 16/577,634.
Notice of Allowance, dated Nov. 3, 2020, from corresponding U.S. Appl. No. 16/719,071.
Notice of Allowance, dated Nov. 5, 2019, from corresponding U.S. Appl. No. 16/560,965.
Notice of Allowance, dated Nov. 7, 2017, from corresponding U.S. Appl. No. 15/671,073.
Notice of Allowance, dated Nov. 8, 2018, from corresponding U.S. Appl. No. 16/042,642.
Notice of Allowance, dated Nov. 9, 2020, from corresponding U.S. Appl. No. 16/595,342.
Notice of Allowance, dated Oct. 1, 2021, from corresponding U.S. Appl. No. 17/340,395.
Notice of Allowance, dated Oct. 10, 2019, from corresponding U.S. Appl. No. 16/277,539.
Notice of Allowance, dated Oct. 17, 2018, from corresponding U.S. Appl. No. 15/896,790.
Notice of Allowance, dated Oct. 17, 2018, from corresponding U.S. Appl. No. 16/054,672.
Notice of Allowance, dated Oct. 17, 2019, from corresponding U.S. Appl. No. 16/563,741.
Notice of Allowance, dated Oct. 21, 2019, from corresponding U.S. Appl. No. 16/404,405.
Notice of Allowance, dated Oct. 21, 2020, from corresponding U.S. Appl. No. 16/834,812.
Notice of Allowance, dated Oct. 22, 2021, from corresponding U.S. Appl. No. 17/346,847.
Notice of Allowance, dated Oct. 3, 2019, from corresponding U.S. Appl. No. 16/511,700.
Notice of Allowance, dated Sep. 1, 2021, from corresponding U.S. Appl. No. 17/196,570.
Notice of Allowance, dated Sep. 1, 2021, from corresponding U.S. Appl. No. 17/222,556.
Notice of Allowance, dated Sep. 12, 2019, from corresponding U.S. Appl. No. 16/512,011.
Notice of Allowance, dated Sep. 13, 2018, from corresponding U.S. Appl. No. 15/894,809.
Notice of Allowance, dated Sep. 13, 2018, from corresponding U.S. Appl. No. 15/894,890.
Notice of Allowance, dated Sep. 14, 2021, from corresponding U.S. Appl. No. 16/808,497.
Notice of Allowance, dated Sep. 16, 2020, from corresponding U.S. Appl. No. 16/915,097.
Notice of Allowance, dated Sep. 17, 2020, from corresponding U.S. Appl. No. 16/863,226.
Office Action, dated Sep. 11, 2017, from corresponding U.S. Appl. No. 15/619,478.
Office Action, dated Sep. 15, 2021, from corresponding U.S. Appl. No. 16/623,157.
Office Action, dated Sep. 16, 2019, from corresponding U.S. Appl. No. 16/277,715.
Office Action, dated Sep. 19, 2017, from corresponding U.S. Appl. No. 15/671,073.
Office Action, dated Sep. 22, 2017, from corresponding U.S. Appl. No. 15/619,278.
Office Action, dated Sep. 24, 2021, from corresponding U.S. Appl. No. 17/342,153.
Office Action, dated Sep. 4, 2020, from corresponding U.S. Appl. No. 16/989,086.
Office Action, dated Sep. 5, 2017, from corresponding U.S. Appl. No. 15/619,469.

(56) **References Cited**

OTHER PUBLICATIONS

Office Action, dated Sep. 6, 2017, from corresponding U.S. Appl. No. 15/619,479.
Office Action, dated Sep. 7, 2017, from corresponding U.S. Appl. No. 15/633,703.
Office Action, dated Sep. 8, 2017, from corresponding U.S. Appl. No. 15/619,251.
Notice of Allowance, dated Apr. 12, 2017, from corresponding U.S. Appl. No. 15/256,419.
Notice of Allowance, dated Apr. 12, 2022, from corresponding U.S. Appl. No. 17/479,807.
Notice of Allowance, dated Apr. 14, 2022, from corresponding U.S. Appl. No. 17/572,276.
Notice of Allowance, dated Apr. 17, 2020, from corresponding U.S. Appl. No. 16/593,639.
Notice of Allowance, dated Apr. 19, 2021, from corresponding U.S. Appl. No. 17/164,029.
Notice of Allowance, dated Apr. 2, 2019, from corresponding U.S. Appl. No. 16/160,577.
Notice of Allowance, dated Apr. 2, 2021, from corresponding U.S. Appl. No. 17/162,006.
Notice of Allowance, dated Apr. 20, 2022, from corresponding U.S. Appl. No. 17/573,808.
Notice of Allowance, dated Apr. 22, 2021, from corresponding U.S. Appl. No. 17/163,701.
Notice of Allowance, dated Apr. 25, 2018, from corresponding U.S. Appl. No. 15/883,041.
Notice of Allowance, dated Apr. 27, 2022, from corresponding U.S. Appl. No. 17/573,999.
Notice of Allowance, dated Apr. 28, 2021, from corresponding U.S. Appl. No. 17/135,445.
Notice of Allowance, dated Apr. 28, 2021, from corresponding U.S. Appl. No. 17/181,828.
Notice of Allowance, dated Apr. 28, 2022, from corresponding U.S. Appl. No. 17/592,922.
Notice of Allowance, dated Apr. 28, 2022, from corresponding U.S. Appl. No. 17/670,352.
Notice of Allowance, dated Apr. 29, 2020, from corresponding U.S. Appl. No. 16/700,049.
Notice of Allowance, dated Apr. 29, 2022, from corresponding U.S. Appl. No. 17/387,421.
Notice of Allowance, dated Apr. 30, 2020, from corresponding U.S. Appl. No. 16/565,265.
Notice of Allowance, dated Apr. 30, 2020, from corresponding U.S. Appl. No. 16/820,346.
Notice of Allowance, dated Apr. 30, 2021, from corresponding U.S. Appl. No. 16/410,762.
Notice of Allowance, dated Apr. 4, 2022, from corresponding U.S. Appl. No. 17/493,332.
Notice of Allowance, dated Apr. 4, 2022, from corresponding U.S. Appl. No. 17/572,298.
Notice of Allowance, dated Apr. 8, 2019, from corresponding U.S. Appl. No. 16/228,250.
Notice of Allowance, dated Apr. 8, 2020, from corresponding U.S. Appl. No. 16/791,348.
Notice of Allowance, dated Apr. 9, 2020, from corresponding U.S. Appl. No. 16/791,075.
Notice of Allowance, dated Aug. 10, 2020, from corresponding U.S. Appl. No. 16/671,444.
Notice of Allowance, dated Aug. 10, 2020, from corresponding U.S. Appl. No. 16/788,633.
Notice of Allowance, dated Aug. 12, 2020, from corresponding U.S. Appl. No. 16/719,488.
Notice of Allowance, dated Aug. 12, 2021, from corresponding U.S. Appl. No. 16/881,832.
Notice of Allowance, dated Aug. 14, 2018, from corresponding U.S. Appl. No. 15/989,416.
Notice of Allowance, dated Aug. 18, 2017, from corresponding U.S. Appl. No. 15/619,455.
Notice of Allowance, dated Aug. 20, 2019, from corresponding U.S. Appl. No. 16/241,710.
Notice of Allowance, dated Aug. 24, 2018, from corresponding U.S. Appl. No. 15/619,479.
Notice of Allowance, dated Aug. 26, 2019, from corresponding U.S. Appl. No. 16/443,374.
Notice of Allowance, dated Aug. 26, 2020, from corresponding U.S. Appl. No. 16/808,503.
Notice of Allowance, dated Aug. 28, 2019, from corresponding U.S. Appl. No. 16/278,120.
Notice of Allowance, dated Aug. 30, 2018, from corresponding U.S. Appl. No. 15/996,208.
Notice of Allowance, dated Aug. 31, 2021, from corresponding U.S. Appl. No. 17/326,901.
Notice of Allowance, dated Aug. 4, 2021, from corresponding U.S. Appl. No. 16/895,278.
AvePoint, Automating Privacy Impact Assessments, AvePoint, Inc.
AvePoint, AvePoint Privacy Impact Assessment 1: User Guide, Cumulative Update 2, Revision E, Feb. 2015, AvePoint, Inc.
Ball, et al, "Aspects of the Computer-Based Patient Record," Computers in Healthcare, Springer-Verlag New York Inc., pp. 1-23 (Year: 1992).
Banerjee et al, "Link Before You Share: Managing Privacy Policies through Blockchain," IEEE, pp. 4438-4447 (Year: 2017).
Barker, "Personalizing Access Control by Generalizing Access Control," ACM, pp. 149-158 (Year: 2010).
Barr, "Amazon Rekognition Update—Estimated Age Range for Faces," AWS News Blog, Feb. 10, 2017, pp. 1-5 (Year: 2017).
Bayardo et al, "Technological Solutions for Protecting Privacy," Computer 36.9 (2003), pp. 115-118, (Year: 2003).
Berezovskiy et al, "A framework for dynamic data source identification and orchestration on the Web", ACM, pp. 1-8 (Year: 2010).
Bertino et al, "On Specifying Security Policies for Web Documents with an XML-based Language," ACM, pp. 57-65 (Year: 2001).
Bertino et al, "Towards Mechanisms for Detection and Prevention of Data Exfiltration by Insiders," Mar. 22, 2011, ACM, pp. 10-19 (Year: 2011).
Bhargav-Spantzel et al., Receipt Management—Transaction History based Trust Establishment, 2007, ACM, p. 82-91.
Bhuvaneswaran et al, "Redundant Parallel Data Transfer Schemes for the Grid Environment", ACM, pp. 18 (Year: 2006).
Bieker, et al, "Privacy-Preserving Authentication Solutions—Best Practices for Implementation and EU Regulatory Perspectives," Oct. 29, 2014, IEEE, pp. 1-10 (Year: 2014).
Bin, et al, "Research on Data Mining Models for the Internet of Things," IEEE, pp. 1-6 (Year: 2010).
Bjorn Greif, "Cookie Pop-up Blocker: Cliqz Automatically Denies Consent Requests," Cliqz.com, pp. 1-9, Aug. 11, 2019 (Year: 2019).
Borgida, "Description Logics in Data Management," IEEE Transactions on Knowledge and Data Engineering, vol. 7, No. 5, Oct. 1995, pp. 671-682 (Year: 1995).
Brandt et al, "Efficient Metadata Management in Large Distributed Storage Systems," IEEE, pp. 1-9 (Year: 2003).
Bujlow et al, "Web Tracking: Mechanisms, Implications, and Defenses," Proceedings of the IEEE, Aug. 1, 2017, vol. 5, No. 8, pp. 1476-1510 (Year: 2017).
Byun, Ji-Won, Elisa Bertino, and Ninghui Li. "Purpose based access control of complex data for privacy protection." Proceedings of the tenth ACM symposium on Access control models and technologies. ACM, 2005. (Year: 2005).
Carminati et al, "Enforcing Access Control Over Data Streams," ACM, pp. 21-30 (Year: 2007).
Carpineto et al, "Automatic Assessment of Website Compliance to the European Cookie Law with CooLCheck," Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, 2016, pp. 135-138 (Year: 2016).
Cerpzone, "How to Access Data on Data Archival Storage and Recovery System", https://www.saj.usace.army.mil/Portals/44/docs/Environmental/Lake%20O%20Watershed/15February2017/How%20To%20Access%20Model%20Data%20on%20DASR.pdf?ver=2017-02-16-095535-633, Feb. 16, 2017.
Cha et al, "A Data-Driven Security Risk Assessment Scheme for Personal Data Protection," IEEE, pp. 50510-50517 (Year: 2018).

(56) **References Cited**

OTHER PUBLICATIONS

Cha, et al, "Process-Oriented Approach for Validating Asset Value for Evaluating Information Security Risk," IEEE, Aug. 31, 2009, pp. 379-385 (Year: 2009).
Chang et al, "A Ranking Approach for Human Age Estimation Based on Face Images," IEEE, 2010, pp. 3396-3399 (Year: 2010).
Chapados et al, "Scoring Models for Insurance Risk Sharing Pool Optimization," 2008, IEEE, pp. 97-105 (Year: 2008).
Cheng, Raymond, et al, "Radiatus: A Shared-Nothing Server-Side Web Architecture," Proceedings of the Seventh ACM Symposium on Cloud Computing, Oct. 5, 2016, pp. 237-250 (Year: 2016).
Choi et al, "Retrieval Effectiveness of Table of Contents and Subject Headings," ACM, pp. 103-104 (Year: 2007).
Chowdhury et al, "A System Architecture for Subject-Centric Data Sharing", ACM, pp. 1-10 (Year: 2018).
Chowdhury et al, "Managing Data Transfers in Computer Clusters with Orchestra," ACM, pp. 98-109 (Year: 2011).
Civili et al, "Mastro Studio: Managing Ontology-Based Data Access Applications," ACM, pp. 1314-1317, Aug. 26-30, 2013 (Year: 2013).
Decision Regarding Institution of Post-Grant Review in Case PGR2018-00056 for U.S. Pat. No. 9,691,090 B1, Oct. 11, 2018.
Degeling et al, "We Value Your Privacy . . . Now Take Some Cookies: Measuring the GDPRs Impact on Web Privacy," arxiv.org, Cornell University Library, 201 Olin Library Cornell University, Ithaca, NY 14853, Aug. 15, 2018, pp. 1-15 (Year: 2019).
Dimou et al, "Machine-Interpretable Dataset and Service Descriptions for Heterogeneous Data Access and Retrieval", ACM, pp. 145-152 (Year: 2015).
Dokholyan et al, "Regulatory and Ethical Considerations for Linking Clinical and Administrative Databases," American Heart Journal 157.6 (2009), pp. 971-982 (Year: 2009).
Dunkel et al, "Data Organization and Access for Efficient Data Mining", IEEE, pp. 522-529 (Year: 1999).
Dwork, Cynthia, Differential Privacy, Microsoft Research, p. 1-12.
Edinger et al, "Age and Gender Estimation of Unfiltered Faces," IEEE, 2014, pp. 2170-2179 (Year: 2014).
Emerson, et al, "A Data Mining Driven Risk Profiling Method for Road Asset Management," ACM, pp. 1267-1275 (Year: 2013).
Enck, William, et al, TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, ACM Transactions on Computer Systems, vol. 32, No. 2, Article 5, Jun. 2014, p. 5:1-5:29.
Everypixel Team, "A New Age Recognition API Detects the Age of People on Photos," May 20, 2019, pp. 1-5 (Year: 2019).
Fan et al, "Intrusion Investigations with Data-hiding for Computer Log-file Forensics," IEEE, pp. 1-6 (Year: 2010).
Final Written Decision Regarding Post-Grant Review in Case PGR2018-00056 for U.S. Pat. No. 9,691,090 B1, Oct. 10, 2019.
Francis, Andre, Business Mathematics and Statistics, South-Western Cengage Learning, 2008, Sixth Edition.
Friedman et al, "Data Mining with Differential Privacy," ACM, Jul. 2010, pp. 493-502 (Year: 2010).
Frikken, Keith B., et al, Yet Another Privacy Metric for Publishing Micro-data, Miami University, Oct. 27, 2008, p. 117-121.
Fung et al, "Discover Information and Knowledge from Websites using an Integrated Summarization and Visualization Framework", IEEE, pp. 232-235 (Year: 2010).
Gajare et al, "Improved Automatic Feature Selection Approach for Health Risk Prediction," Feb. 16, 2018, IEEE, pp. 816-819 (Year: 2018).
Geko et al, "An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security," ACM, pp. 1-6, Nov. 15-16, 2018 (Year: 2018).
Golab, et al, "Issues in Data Stream Management," ACM, SIGMOD Record, vol. 32, No. 2, Jun. 2003, pp. 5-14 (Year: 2003).
Office Action, dated Aug. 27, 2021, from corresponding U.S. Appl. No. 17/187,329.
Office Action, dated Aug. 27, 2021, from corresponding U.S. Appl. No. 17/334,948.
Office Action, dated Aug. 29, 2017, from corresponding U.S. Appl. No. 15/619,237.
Office Action, dated Aug. 30, 2017, from corresponding U.S. Appl. No. 15/619,212.
Office Action, dated Aug. 30, 2017, from corresponding U.S. Appl. No. 15/619,382.
Office Action, dated Aug. 30, 2021, from corresponding U.S. Appl. No. 16/938,520.
Office Action, dated Aug. 6, 2019, from corresponding U.S. Appl. No. 16/404,491.
Office Action, dated Aug. 6, 2020, from corresponding U.S. Appl. No. 16/862,956.
Office Action, dated Dec. 11, 2019, from corresponding U.S. Appl. No. 16/578,712.
Office Action, dated Dec. 13, 2021, from corresponding U.S. Appl. No. 17/476,209.
Office Action, dated Dec. 14, 2018, from corresponding U.S. Appl. No. 16/104,393.
Office Action, dated Dec. 15, 2016, from corresponding U.S. Appl. No. 15/256,419.
Office Action, dated Dec. 16, 2019, from corresponding U.S. Appl. No. 16/563,754.
Office Action, dated Dec. 16, 2019, from corresponding U.S. Appl. No. 16/565,265.
Office Action, dated Dec. 16, 2020, from corresponding U.S. Appl. No. 17/020,275.
Office Action, dated Dec. 17, 2021, from corresponding U.S. Appl. No. 17/395,759.
Office Action, dated Dec. 17, 2021, from corresponding U.S. Appl. No. 17/499,582.
Office Action, dated Dec. 18, 2020, from corresponding U.S. Appl. No. 17/030,714.
Office Action, dated Dec. 19, 2019, from corresponding U.S. Appl. No. 16/410,866.
Office Action, dated Dec. 2, 2019, from corresponding U.S. Appl. No. 16/560,963.
Office Action, dated Dec. 2, 2021, from corresponding U.S. Appl. No. 17/504,102.
Office Action, dated Dec. 23, 2019, from corresponding U.S. Appl. No. 16/593,639.
Office Action, dated Dec. 24, 2020, from corresponding U.S. Appl. No. 17/068,454.
Office Action, dated Dec. 27, 2021, from corresponding U.S. Appl. No. 17/493,332.
Office Action, dated Dec. 29, 2021, from corresponding U.S. Appl. No. 17/479,807.
Office Action, dated Dec. 3, 2018, from corresponding U.S. Appl. No. 16/055,998.
Office Action, dated Dec. 30, 2021, from corresponding U.S. Appl. No. 17/149,421.
Office Action, dated Dec. 31, 2018, from corresponding U.S. Appl. No. 16/160,577.
Office Action, dated Dec. 7, 2021, from corresponding U.S. Appl. No. 17/499,609.
Office Action, dated Dec. 8, 2020, from corresponding U.S. Appl. No. 17/013,758.
Office Action, dated Dec. 8, 2020, from corresponding U.S. Appl. No. 17/068,198.
Office Action, dated Feb. 10, 2021, from corresponding U.S. Appl. No. 16/862,944.
Office Action, dated Feb. 10, 2021, from corresponding U.S. Appl. No. 17/106,469.
Office Action, dated Feb. 15, 2019, from corresponding U.S. Appl. No. 16/220,899.
Office Action, dated Feb. 16, 2022, from corresponding U.S. Appl. No. 16/872,031.
Office Action, dated Feb. 17, 2021, from corresponding U.S. Appl. No. 16/862,948.
Office Action, dated Feb. 18, 2021, from corresponding U.S. Appl. No. 16/862,952.
Office Action, dated Feb. 2, 2021, from corresponding U.S. Appl. No. 17/101,915.

(56) **References Cited**

OTHER PUBLICATIONS

Office Action, dated Feb. 26, 2019, from corresponding U.S. Appl. No. 16/228,250.
Office Action, dated Feb. 3, 2021, from corresponding U.S. Appl. No. 17/013,757.
Office Action, dated Feb. 5, 2020, from corresponding U.S. Appl. No. 16/586,202.
Office Action, dated Feb. 6, 2020, from corresponding U.S. Appl. No. 16/707,762.
Office Action, dated Feb. 8, 2021, from corresponding U.S. Appl. No. 17/139,650.
Office Action, dated Feb. 9, 2021, from corresponding U.S. Appl. No. 16/808,493.
Office Action, dated Feb. 9, 2022, from corresponding U.S. Appl. No. 17/543,546.
Office Action, dated Jan. 14, 2022, from corresponding U.S. Appl. No. 17/499,595.
Office Action, dated Jan. 18, 2019, from corresponding U.S. Appl. No. 16/055,984.
Office Action, dated Jan. 21, 2022, from corresponding U.S. Appl. No. 17/499,624.
Office Action, dated Jan. 22, 2021, from corresponding U.S. Appl. No. 17/099,270.
Office Action, dated Jan. 24, 2020, from corresponding U.S. Appl. No. 16/505,426.
Office Action, dated May 14, 2020, from corresponding U.S. Appl. No. 16/808,497.
Office Action, dated May 14, 2020, from corresponding U.S. Appl. No. 16/808,503.
Office Action, dated May 15, 2020, from corresponding U.S. Appl. No. 16/808,493.
Office Action, dated May 16, 2018, from corresponding U.S. Appl. No. 15/882,989.
Office Action, dated May 16, 2022, from corresponding U.S. Appl. No. 17/679,750.
Office Action, dated May 17, 2019, from corresponding U.S. Appl. No. 16/277,539.
Office Action, dated May 18, 2021, from corresponding U.S. Appl. No. 17/196,570.
Office Action, dated May 2, 2018, from corresponding U.S. Appl. No. 15/894,809.
Office Action, dated May 2, 2019, from corresponding U.S. Appl. No. 16/104,628.
Office Action, dated May 29, 2020, from corresponding U.S. Appl. No. 16/862,944.
Office Action, dated May 29, 2020, from corresponding U.S. Appl. No. 16/862,948.
Office Action, dated May 29, 2020, from corresponding U.S. Appl. No. 16/863,226.
Office Action, dated May 5, 2020, from corresponding U.S. Appl. No. 16/410,336.
Office Action, dated May 9, 2022, from corresponding U.S. Appl. No. 16/840,943.
Office Action, dated Nov. 1, 2017, from corresponding U.S. Appl. No. 15/169,658.
Office Action, dated Nov. 10, 2021, from corresponding U.S. Appl. No. 17/380,485.
Office Action, dated Nov. 10, 2021, from corresponding U.S. Appl. No. 17/409,999.
Office Action, dated Nov. 12, 2020, from corresponding U.S. Appl. No. 17/034,355.
Office Action, dated Nov. 12, 2020, from corresponding U.S. Appl. No. 17/034,772.
Office Action, dated Nov. 12, 2021, from corresponding U.S. Appl. No. 17/346,586.
Office Action, dated Nov. 12, 2021, from corresponding U.S. Appl. No. 17/373,444.
Office Action, dated Nov. 15, 2018, from corresponding U.S. Appl. No. 16/059,911.
Office Action, dated Nov. 15, 2019, from corresponding U.S. Appl. No. 16/552,758.
Office Action, dated Nov. 16, 2021, from corresponding U.S. Appl. No. 17/370,650.
Office Action, dated Nov. 16, 2021, from corresponding U.S. Appl. No. 17/486,350.
Office Action, dated Nov. 18, 2019, from corresponding U.S. Appl. No. 16/560,885.
Office Action, dated Nov. 18, 2019, from corresponding U.S. Appl. No. 16/560,889.
Office Action, dated Nov. 18, 2019, from corresponding U.S. Appl. No. 16/572,347.
Office Action, dated Nov. 19, 2019, from corresponding U.S. Appl. No. 16/595,342.
Office Action, dated Nov. 20, 2019, from corresponding U.S. Appl. No. 16/595,327.
Office Action, dated Nov. 23, 2018, from corresponding U.S. Appl. No. 16/042,673.
Office Action, dated Nov. 23, 2021, from corresponding U.S. Appl. No. 17/013,756.
Office Action, dated Nov. 24, 2020, from corresponding U.S. Appl. No. 16/925,628.
Office Action, dated Nov. 26, 2021, from corresponding U.S. Appl. No. 16/925,550.
Office Action, dated Nov. 4, 2021, from corresponding U.S. Appl. No. 17/491,906.
Office Action, dated Nov. 8, 2021, from corresponding U.S. Appl. No. 16/872,130.
Office Action, dated Oct. 10, 2018, from corresponding U.S. Appl. No. 16/041,563.
Office Action, dated Oct. 10, 2018, from corresponding U.S. Appl. No. 16/055,083.
Office Action, dated Oct. 10, 2018, from corresponding U.S. Appl. No. 16/055,944.
Office Action, dated Oct. 12, 2021, from corresponding U.S. Appl. No. 17/346,509.
Office Action, dated Oct. 14, 2020, from corresponding U.S. Appl. No. 16/927,658.
Office Action, dated Oct. 15, 2018, from corresponding U.S. Appl. No. 16/054,780.
Office Action, dated Oct. 15, 2021, from corresponding U.S. Appl. No. 16/908,081.
Office Action, dated Oct. 16, 2019, from corresponding U.S. Appl. No. 16/557,392.
Office Action, dated Oct. 16, 2020, from corresponding U.S. Appl. No. 16/808,489.
Office Action, dated Oct. 23, 2018, from corresponding U.S. Appl. No. 16/055,961.
Office Action, dated Oct. 26, 2018, from corresponding U.S. Appl. No. 16/041,468.
Office Action, dated Oct. 8, 2019, from corresponding U.S. Appl. No. 16/552,765.
Office Action, dated Sep. 1, 2017, from corresponding U.S. Appl. No. 15/619,459.
Office Action, dated Sep. 11, 2017, from corresponding U.S. Appl. No. 15/619,375.
Office Action, dated Jan. 24, 2020, from corresponding U.S. Appl. No. 16/700,049.
Office Action, dated Jan. 25, 2022, from corresponding U.S. Appl. No. 17/494,220.
Office Action, dated Jan. 27, 2020, from corresponding U.S. Appl. No. 16/656,895.
Office Action, dated Jan. 28. 2020, from corresponding U.S. Appl. No. 16/712,104.
Office Action, dated Jan. 29, 2021, from corresponding U.S. Appl. No. 17/101,106.
Office Action, dated Jan. 31, 2022, from corresponding U.S. Appl. No. 17/493,290.
Office Action, dated Jan. 4, 2019, from corresponding U.S. Appl. No. 16/159,566.
Office Action, dated Jan. 4, 2019, from corresponding U.S. Appl. No. 16/159,628.

(56) **References Cited**

OTHER PUBLICATIONS

Office Action, dated Jan. 4, 2021, from corresponding U.S. Appl. No. 17/013,756.
Office Action, dated Jan. 4, 2022, from corresponding U.S. Appl. No. 17/480,377.
Office Action, dated Jan. 7, 2020, from corresponding U.S. Appl. No. 16/572,182.
Office Action, dated Jan. 7, 2022, from corresponding U.S. Appl. No. 17/387,421.
Office Action, dated Jul. 13, 2021, from corresponding U.S. Appl. No. 17/306,496.
Office Action, dated Jul. 15, 2021, from corresponding U.S. Appl. No. 17/020,275.
Office Action, dated Jul. 18, 2019, from corresponding U.S. Appl. No. 16/410,762.
Office Action, dated Jul. 19, 2021, from corresponding U.S. Appl. No. 17/316,179.
Office Action, dated Jul. 21, 2017, from corresponding U.S. Appl. No. 15/256,430.
Office Action, dated Jul. 21, 2021, from corresponding U.S. Appl. No. 16/901,654.
Office Action, dated Jul. 23, 2019, from corresponding U.S. Appl. No. 16/436,616.
Office Action, dated Jul. 24, 2020, from corresponding U.S. Appl. No. 16/404,491.
Office Action, dated Jul. 27, 2020, from corresponding U.S. Appl. No. 16/595,342.
Office Action, dated Jun. 1, 2020, from corresponding U.S. Appl. No. 16/862,952.
Office Action, dated Jun. 24, 2019, from corresponding U.S. Appl. No. 16/410,336.
Office Action, dated Jun. 24, 2021, from corresponding U.S. Appl. No. 17/234,205.
Office Action, dated Jun. 27, 2019, from corresponding U.S. Appl. No. 16/404,405.
Office Action, dated Jun. 7, 2021, from corresponding U.S. Appl. No. 17/200,698.
Office Action, dated Jun. 9, 2021, from corresponding U.S. Appl. No. 17/222,523.
Office Action, dated Mar. 1, 2022, from corresponding U.S. Appl. No. 17/119,080.
Office Action, dated Mar. 11, 2019, from corresponding U.S. Appl. No. 16/220,978.
Office Action, dated Mar. 12, 2019, from corresponding U.S. Appl. No. 16/221,153.
Office Action, dated Mar. 15, 2021, from corresponding U.S. Appl. No. 17/149,421.
Office Action, dated Mar. 16, 2020, from corresponding U.S. Appl. No. 16/719,488.
Office Action, dated Mar. 17, 2020, from corresponding U.S. Appl. No. 16/565,395.
Office Action, dated Mar. 17, 2020, from corresponding U.S. Appl. No. 16/719,071.
Office Action, dated Mar. 2, 2022, from corresponding U.S. Appl. No. 17/020,275.
Office Action, dated Mar. 2, 2022, from corresponding U.S. Appl. No. 17/161,159.
Office Action, dated Mar. 2, 2022, from corresponding U.S. Appl. No. 17/200,698.
Office Action, dated Mar. 20, 2020, from corresponding U.S. Appl. No. 16/778,709.
Office Action, dated Mar. 21, 2022, from corresponding U.S. Appl. No. 17/571,871.
Office Action, dated Mar. 22, 2022, from corresponding U.S. Appl. No. 17/187,329.
Office Action, dated Mar. 23, 2020, from corresponding U.S. Appl. No. 16/671,444.
Office Action, dated Mar. 25, 2019, from corresponding U.S. Appl. No. 16/278,121.
Office Action, dated Mar. 25, 2020, from corresponding U.S. Appl. No. 16/701,043.
Office Action, dated Mar. 25, 2020, from corresponding U.S. Appl. No. 16/791,006.
Office Action, dated Mar. 27, 2019, from corresponding U.S. Appl. No. 16/278,120.
Office Action, dated Mar. 30, 2018, from corresponding U.S. Appl. No. 15/894,890.
Office Action, dated Mar. 30, 2018, from corresponding U.S. Appl. No. 15/896,790.
Office Action, dated Mar. 30, 2021, from corresponding U.S. Appl. No. 17/151,399.
Office Action, dated Mar. 4, 2019, from corresponding U.S. Appl. No. 16/237,083.
Office Action, dated May 12, 2022, from corresponding U.S. Appl. No. 17/509,974.
Notice of Allowance, dated Aug. 7, 2020, from corresponding U.S. Appl. No. 16/901,973.
Notice of Allowance, dated Aug. 9, 2018, from corresponding U.S. Appl. No. 15/882,989.
Notice of Allowance, dated Aug. 9, 2021, from corresponding U.S. Appl. No. 16/881,699.
Notice of Allowance, dated Dec. 10, 2018, from corresponding U.S. Appl. No. 16/105,602.
Notice of Allowance, dated Dec. 11, 2019, from corresponding U.S. Appl. No. 16/278,122.
Notice of Allowance, dated Dec. 11, 2019, from corresponding U.S. Appl. No. 16/593,634.
Notice of Allowance, dated Dec. 12, 2017, from corresponding U.S. Appl. No. 15/169,643.
Notice of Allowance, dated Dec. 12, 2017, from corresponding U.S. Appl. No. 15/619,212.
Notice of Allowance, dated Dec. 12, 2017, from corresponding U.S. Appl. No. 15/619,382.
Notice of Allowance, dated Dec. 13, 2019, from corresponding U.S. Appl. No. 16/512,033.
Notice of Allowance, dated Dec. 13, 2021, from corresponding U.S. Appl. No. 16/908,081.
Notice of Allowance, dated Dec. 13, 2021, from corresponding U.S. Appl. No. 17/347,853.
Notice of Allowance, dated Dec. 15, 2020, from corresponding U.S. Appl. No. 16/989,086.
Notice of Allowance, dated Dec. 16, 2019, from corresponding U.S. Appl. No. 16/505,461.
Notice of Allowance, dated Dec. 17, 2020, from corresponding U.S. Appl. No. 17/034,772.
Notice of Allowance, dated Dec. 18, 2019, from corresponding U.S. Appl. No. 16/659,437.
Notice of Allowance, dated Dec. 2, 2021, from corresponding U.S. Appl. No. 16/901,654.
Notice of Allowance, dated Dec. 23, 2019, from corresponding U.S. Appl. No. 16/656,835.
Notice of Allowance, dated Dec. 23, 2020, from corresponding U.S. Appl. No. 17/068,557.
Notice of Allowance, dated Dec. 3, 2019, from corresponding U.S. Appl. No. 16/563,749.
Notice of Allowance, dated Dec. 30, 2021, from corresponding U.S. Appl. No. 16/938,520.
Notice of Allowance, dated Dec. 31, 2018, from corresponding U.S. Appl. No. 16/159,634.
Notice of Allowance, dated Dec. 31, 2019, from corresponding U.S. Appl. No. 16/404,399.
Notice of Allowance, dated Dec. 4, 2019, from corresponding U.S. Appl. No. 16/594,670.
Notice of Allowance, dated Dec. 5, 2017, from corresponding U.S. Appl. No. 15/633,703.
Notice of Allowance, dated Dec. 6, 2017, from corresponding U.S. Appl. No. 15/619,451.
Notice of Allowance, dated Dec. 6, 2017, from corresponding U.S. Appl. No. 15/619,459.
Notice of Allowance, dated Dec. 7, 2020, from corresponding U.S. Appl. No. 16/817,136.

(56) **References Cited**

OTHER PUBLICATIONS

Notice of Allowance, dated Dec. 8, 2021, from corresponding U.S. Appl. No. 17/397,472.
Notice of Allowance, dated Dec. 9, 2019, from corresponding U.S. Appl. No. 16/565,261.
Notice of Allowance, dated Dec. 9, 2020, from corresponding U.S. Appl. No. 16/404,491.
Notice of Allowance, dated Feb. 1, 2022, from corresponding U.S. Appl. No. 17/346,509.
Notice of Allowance, dated Feb. 10, 2020, from corresponding U.S. Appl. No. 16/552,765.
Notice of Allowance, dated Feb. 11, 2021, from corresponding U.S. Appl. No. 17/086,732.
Notice of Allowance, dated Feb. 12, 2020, from corresponding U.S. Appl. No. 16/572,182.
Notice of Allowance, dated Feb. 13, 2019, from corresponding U.S. Appl. No. 16/041,563.
Notice of Allowance, dated Feb. 14, 2019, from corresponding U.S. Appl. No. 16/226,272.
Notice of Allowance, dated Feb. 14, 2022, from corresponding U.S. Appl. No. 16/623,157.
Notice of Allowance, dated Feb. 19, 2019, from corresponding U.S. Appl. No. 16/159,632.
Notice of Allowance, dated Feb. 19, 2021, from corresponding U.S. Appl. No. 16/832,451.
Notice of Allowance, dated Feb. 22, 2022, from corresponding U.S. Appl. No. 17/535,065.
Notice of Allowance, dated Feb. 24, 2021, from corresponding U.S. Appl. No. 17/034,355.
Notice of Allowance, dated Feb. 24, 2021, from corresponding U.S. Appl. No. 17/068,198.
Notice of Allowance, dated Feb. 24, 2021, from corresponding U.S. Appl. No. 17/101,106.
Notice of Allowance, dated Feb. 24, 2021, from corresponding U.S. Appl. No. 17/101,253.
Notice of Allowance, dated Feb. 24, 2022, from corresponding U.S. Appl. No. 17/234,205.
Notice of Allowance, dated Feb. 24, 2022, from corresponding U.S. Appl. No. 17/549,170.
Notice of Allowance, dated Feb. 25, 2020, from corresponding U.S. Appl. No. 16/714,355.
Notice of Allowance, dated Feb. 25, 2021, from corresponding U.S. Appl. No. 17/106,469.
Notice of Allowance, dated Feb. 26, 2021, from corresponding U.S. Appl. No. 17/139,650.
Notice of Allowance, dated Sep. 18, 2018, from corresponding U.S. Appl. No. 15/894,819.
Notice of Allowance, dated Sep. 18, 2018, from corresponding U.S. Appl. No. 16/041,545.
Notice of Allowance, dated Sep. 18, 2020, from corresponding U.S. Appl. No. 16/812,795.
Notice of Allowance, dated Sep. 23, 2020, from corresponding U.S. Appl. No. 16/811,793.
Notice of Allowance, dated Sep. 23, 2021, from corresponding U.S. Appl. No. 17/068,454.
Notice of Allowance, dated Sep. 24, 2021, from corresponding U.S. Appl. No. 17/334,939.
Notice of Allowance, dated Sep. 25, 2020, from corresponding U.S. Appl. No. 16/983,536.
Notice of Allowance, dated Sep. 27, 2017, from corresponding U.S. Appl. No. 15/626,052.
Notice of Allowance, dated Sep. 27, 2021, from corresponding U.S. Appl. No. 17/222,523.
Notice of Allowance, dated Sep. 28, 2018, from corresponding U.S. Appl. No. 16/041,520.
Notice of Allowance, dated Sep. 29, 2021, from corresponding U.S. Appl. No. 17/316,179.
Notice of Allowance, dated Sep. 4, 2018, from corresponding U.S. Appl. No. 15/883,041.
Notice of Allowance, dated Sep. 4, 2020, from corresponding U.S. Appl. No. 16/808,500.
Notice of Allowance, dated Sep. 4, 2020, from corresponding U.S. Appl. No. 16/901,662.
Notice of Allowance, dated Sep. 9, 2021, from corresponding U.S. Appl. No. 17/334,909.
Agrawal et al, "Securing Electronic Health Records Without Impeding the Flow of Information," International Journal of Medical Informatics 76, 2007, pp. 471-479 (Year: 2007).
AvePoint, Installing and Configuring the APIA System, International Association of Privacy Professionals, AvePoint, Inc.
Bang et al, "Building an Effective and Efficient Continuous Web Application Security Program," 2016 International Conference on Cyber Security Situational Awareness, Data Analytics and Assessment (CyberSA), London, 2016, pp. 1-4 (Year: 2016).
Binns, et al, "Data Havens, or Privacy Sans Frontières? A Study of International Personal Data Transfers," ACM, pp. 273-274 (Year: 2002).
Czeskis et al, "Lightweight Server Support for Browser-based CSRF Protection," Proceedings of the 22nd International Conference on World Wide Web, 2013, pp. 273-284 (Year: 2013).
Falahrastegar, Marjan, et al, Tracking Personal Identifiers Across the Web, Medical Image Computing and Computer-Assisted Intervention—Miccai 2015, 18th International Conference, Oct. 5, 2015, Munich, Germany.
Friedman et al, "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design," Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002, IEEE, pp. 1-10 (Year: 2002).
Ghiglieri, Marco et al.; Personal DLP for Facebook, 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (Percom Workshops); IEEE; Mar. 24, 2014; pp. 629-634.
Gilda, et al, "Blockchain for Student Data Privacy and Consent," 2018 International Conference on Computer Communication and Informatics, Jan. 4-6, 2018, IEEE, pp. 1-5 (Year: 2018).
Halevy, et al, "Schema Mediation in Peer Data Management Systems," IEEE, Proceedings of the 19th International Conference on Data Engineering, 2003, pp. 505-516 (Year: 2003).
IAPP, Daily Dashboard, PIA Tool Stocked With New Templates for DPI, Infosec, International Association of Privacy Professionals, Apr. 22, 2014.
IAPP, ISO/IEC 27001 Information Security Management Template, Resource Center, International Association of Privacy Professionals.
International Search Report, dated Apr. 12, 2022, from corresponding International Application No. PCT/US2022/016735.
International Search Report, dated Aug. 15, 2017, from corresponding International Application No. PCT/US2017/036919.
International Search Report, dated Aug. 21, 2017, from corresponding International Application No. PCT/US2017/036914.
International Search Report, dated Aug. 29, 2017, from corresponding International Application No. PCT/US2017/036898.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036889.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036890.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036893.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036901.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036913.
International Search Report, dated Aug. 8, 2017, from corresponding International Application No. PCT/US2017/036920.
International Search Report, dated Dec. 14, 2018, from corresponding International Application No. PCT/US2018/045296.
International Search Report, dated Dec. 22, 2021, from corresponding International Application No. PCT/US2021/051217.
International Search Report, dated Feb. 11, 2022, from corresponding International Application No. PCT/US2021/053518.
International Search Report, dated Feb. 14, 2022, from corresponding International Application No. PCT/US2021/058274.

(56) **References Cited**

OTHER PUBLICATIONS

International Search Report, dated Jan. 14, 2019, from corresponding International Application No. PCT/US2018/046949.
International Search Report, dated Jan. 5, 2022, from corresponding International Application No. PCT/US2021/050497.
International Search Report, dated Jan. 7, 2019, from corresponding International Application No. PCT/US2018/055772.
International Search Report, dated Jun. 21, 2017, from corresponding International Application No. PCT/US2017/025600.
International Search Report, dated Jun. 6, 2017, from corresponding International Application No. PCT/US2017/025605.
International Search Report, dated Jun. 6, 2017, from corresponding International Application No. PCT/US2017/025611.
International Search Report, dated Mar. 14, 2019, from corresponding International Application No. PCT/US2018/055736.
International Search Report, dated Mar. 18, 2022, from corresponding International Application No. PCT/US2022/013733.
International Search Report, dated Mar. 4, 2019, from corresponding International Application No. PCT/US2018/055773.
Matte et al, "Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 791-809 (Year: 2020).
McGarth et al, "Digital Library Technology for Locating and Accessing Scientific Data", ACM, pp. 188-194 (Year: 1999).
Mesbah et al, "Crawling Ajax-Based Web Applications Through Dynamic Analysis of User Interface State Changes," ACM Transactions on the Web (TWEB) vol. 6, No. 1, Article 3, Mar. 2012, pp. 1-30 (Year: 2012).
Milic et al, "Comparative Analysis of Metadata Models on e-Government Open Data Platforms," IEEE, pp. 119-130 (Year: 2021).
Moscoso-Zea et al, "Datawarehouse Design for Educational Data Mining," IEEE, pp. 1-6 (Year: 2016).
Mudepalli et al, "An efficient data retrieval approach using blowfish encryption on cloud CipherText Retrieval in Cloud Computing" IEEE, pp. 267-271 (Year: 2017).
Mundada et al, "Half-Baked Cookies: Hardening Cookie-Based Authentication for the Modern Web," Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016, pp. 675-685 (Year: 2016).
Newman et al, "High Speed Scientific Data Transfers using Software Defined Networking," ACM, pp. 1-9 (Year: 2015).
Newman, "Email Archive Overviews using Subject Indexes", ACM, pp. 652-653, 2002 (Year: 2002).
Nishikawa, Taiji, English Translation of JP 2019154505, Aug. 27, 2019 (Year: 2019).
Notice of Filing Date for Petition for Post-Grant Review of related U.S. Pat. No. 9,691,090 dated Apr. 12, 2018.
Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," ACM, pp. 1-13, Apr. 25, 2020 (Year: 2020).
O'Keefe et al, "Privacy-Preserving Data Linkage Protocols," Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, 2004, pp. 94-102 (Year: 2004).
Olenski, Steve, For Consumers, Data Is a Matter of Trust, CMO Network, Apr. 18, 2016, https://www.forbes.com/sites/steveolenski/2016/04/18/for-consumers-data-is-a-matter-of-trust/#2e48496278b3.
Paes, "Student Research Abstract: Automatic Detection of Cross-Browser Incompatibilities using Machine Learning and Screenshot Similarity," ACM, pp. 697-698, Apr. 3, 2017 (Year: 2017).
Pearson, et al, "A Model-Based Privacy Compliance Checker," IJEBR, vol. 5, No. 2, pp. 63-83, 2009, Nov. 21, 2008. [Online]. Available: http://dx.doi.org/10.4018/jebr.2009040104 (Year: 2008).
Pechenizkiy et al, "Process Mining Online Assessment Data," Educational Data Mining, pp. 279-288 (Year: 2009).
Petition for Post-Grant Review of related U.S. Pat. No. 9,691,090 dated Mar. 27, 2018.
Petrie et al, "The Relationship between Accessibility and Usability of Websites", ACM, pp. 397-406 (Year: 2007).
Ping et al, "Wide Area Placement of Data Replicas for Fast and Highly Available Data Access," ACM, pp. 1-8 (Year: 2011).
Popescu-Zeletin, "The Data Access and Transfer Support in a Local Heterogeneous Network (HMINET)", IEEE, pp. 147-152 (Year: 1979).
Porter, "De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information," Shidler JL Com. & Tech. 5, 2008, pp. 1-9 (Year: 2008).
Pretorius, et al, "Attributing Users Based on Web Browser History," 2017 IEEE Conference on Application, Information and Network Security (AINS), 2017, pp. 69-74 (Year: 2017).
Qiu, et al, "Design and Application of Data Integration Platform Based on Web Services and XML," IEEE, pp. 253-256 (Year: 2016).
Qu et al, "Metadata Type System: Integrate Presentation, Data Models and Extraction to Enable Exploratory Browsing Interfaces," ACM, pp. 107-116 (Year: 2014).
Radu, et al, "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods," IEEE, Dec. 12, 2020, pp. 1-6 (Year: 2020).
Rakers, "Managing Professional and Personal Sensitive Information," ACM, pp. 9-13, Oct. 24-27, 2010 (Year: 2010).
Reardon et al., User-Level Secure Deletion on Log Structured File Systems, ACM, 2012, retrieved online on Apr. 22, 2021, pp. 1-11. Retrieved from the Internet: URL: http://citeseerx.ist.psu.edu/viewdoc/download;isessionid=450713515DC7F19F8ED09AE961D4B60E. (Year: 2012).
Regulation (EU) 2016/679, "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Official Journal of the European Union, May 4, 2016, pp. L 119/1-L 119/88 (Year: 2016).
Roesner et al, "Detecting and Defending Against Third-Party Tracking on the Web," 9th USENIX Symposium on Networked Systems Design and Implementation, Apr. 11, 2013, pp. 1-14, ACM (Year: 2013).
Rozepz, "What is Google Privacy Checkup? Everything You Need to Know," Tom's Guide web post, Apr. 26, 2018, pp. 1-11 (Year: 2018).
Sachinopoulou et al, "Ontology-Based Approach for Managing Personal Health and Wellness Information," IEEE, pp. 1802-1805 (Year: 2007).
Salim et al, "Data Retrieval and Security using Lightweight Directory Access Protocol", IEEE, pp. 685-688 (Year: 2009).
Sanchez-Rola et al, "Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control," Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019, pp. 340-351 (Year: 2019).
Santhisree, et al, "Web Usage Data Clustering Using Dbscan Algorithm and Set Similarities," IEEE, pp. 220-224 (Year: 2010).
Sanzo et al, "Analytical Modeling of Lock-Based Concurrency Control with Arbitrary Transaction Data Access Patterns," ACM, pp. 69-78 (Year: 2010).
Sarkar et al, "Towards Enforcement of the EU GDPR: Enabling Data Erasure," 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018, pp. 222-229, IEEE (Year: 2018).
Schwartz, Edward J., et al, 2010 IEEE Symposium on Security and Privacy: All You Ever Wanted to Know About Dynamic Analysis and forward Symbolic Execution (but might have been afraid to ask), Carnegie Mellon University, IEEE Computer Society, 2010, p. 317-331.
Sedinic et al, "Security Risk Management in Complex Organization," May 29, 2015, IEEE, pp. 1331-1337 (Year: 2015).
Shahriar et al, "A Model-Based Detection of Vulnerable and Malicious Browser Extensions," IEEE, pp. 198-207 (Year: 2013).
Shankar et al, "Doppleganger: Better Browser Privacy Without the Bother," Proceedings of the 13th ACM Conference on Computer and Communications Security; [ACM Conference on Computer and Communications Security], New York, NY : ACM, US, Oct. 30, 2006, pp. 154-167 (Year: 2006).

(56) **References Cited**

OTHER PUBLICATIONS

Shulz et al, "Generative Data Models for Validation and Evaluation of Visualization Techniques," ACM, pp. 1-13 (Year: 2016).
Singh, et al, "A Metadata Catalog Service for Data Intensive Applications," ACM, pp. 1-17 (Year: 2003).
Sjosten et al, "Discovering Browser Extensions via Web Accessible Resources," ACM, pp. 329-336, Mar. 22, 2017 (Year: 2017).
Slezak, et al, "Brighthouse: An Analytic Data Warehouse for Ad-hoc Queries," ACM, pp. 1337-1345 (Year: 2008).
Soceanu, et al, "Managing the Privacy and Security of eHealth Data," May 29, 2015, IEEE, pp. 1-8 (Year: 2015).
Srinivasan et al, "Descriptive Data Analysis of File Transfer Data," ACM, pp. 1-8 (Year: 2014).
Stack Overflow, "Is there a way to force a user to scroll to the bottom of a div?," Stack Overflow, pp. 1-11, Nov. 2013. [Online]. Available: https://stackoverflow.com/questions/2745935/is-there-a-way-to-force-a-user-to-scroll-to-the-bottom-of-a-div (Year: 2013).
Stern, Joanna, "iPhone Privacy Is Broken . . . and Apps Are to Blame", The Wall Street Journal, wsj.com, May 31, 2019.
Strodl, et al, "Personal & SOHO Archiving," Vienna University of Technology, Vienna, Austria, JCDL '08, Jun. 16-20, 2008, Pittsburgh, Pennsylvania, USA, pp. 115-123 (Year: 2008).
U.S. Appl. No. 18/110,511, Jul. 22, 2024, Notice of Allowance.
U.S. Appl. No. 17/743,749, Aug. 9, 2024, Notice of Allowance.
U.S. Appl. No. 17/717,587, Aug. 23, 2023, Notice of Allowance.

* cited by examiner

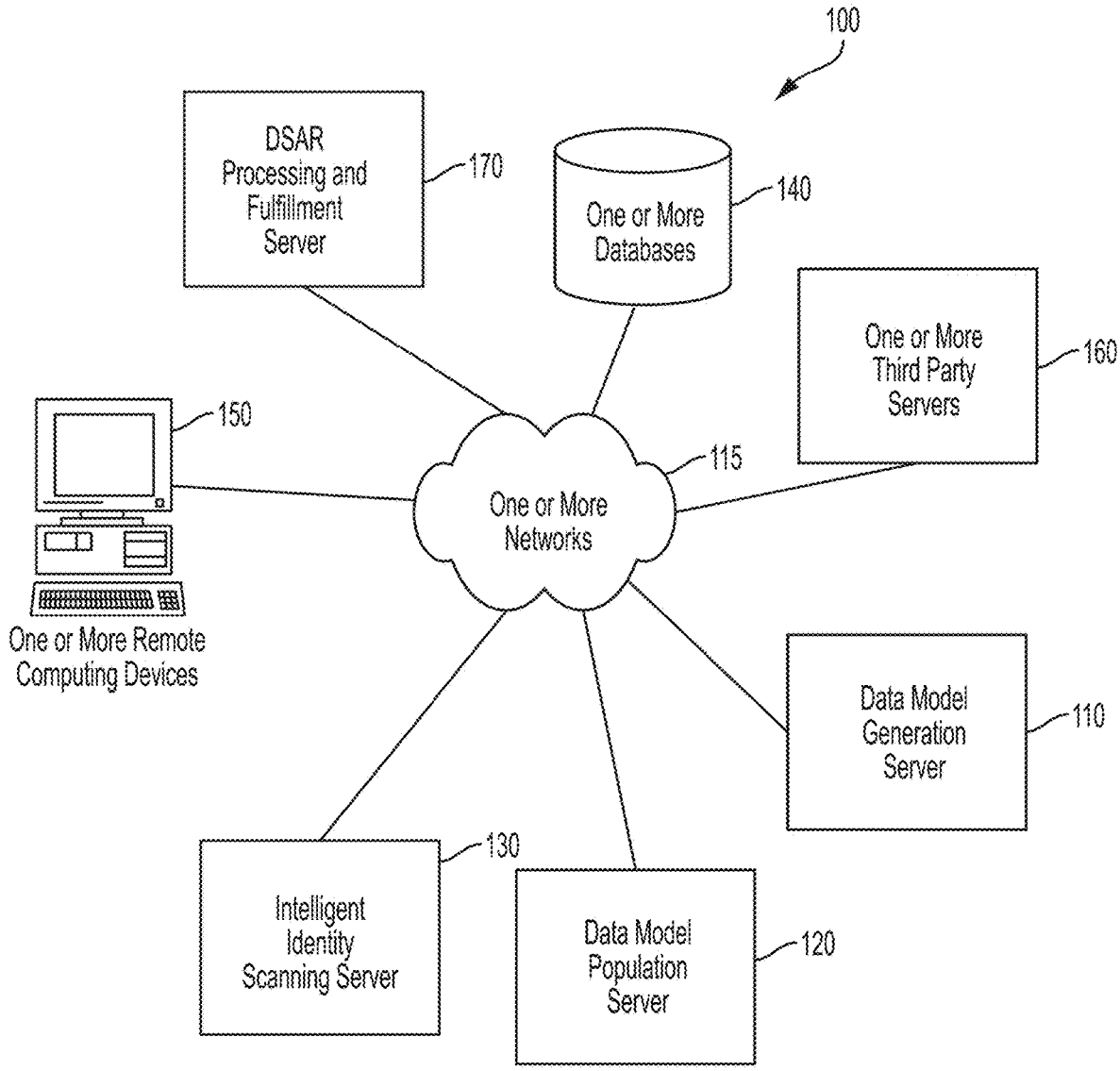

100
DSAR Processing and Fulfillment Server
170
One or More Databases
140
One or More Third Party Servers
160
150
One or More Remote Computing Devices
One or More Networks
115
Data Model Generation Server
110
Intelligent Identity Scanning Server
130
Data Model Population Server
120

FIG. 1

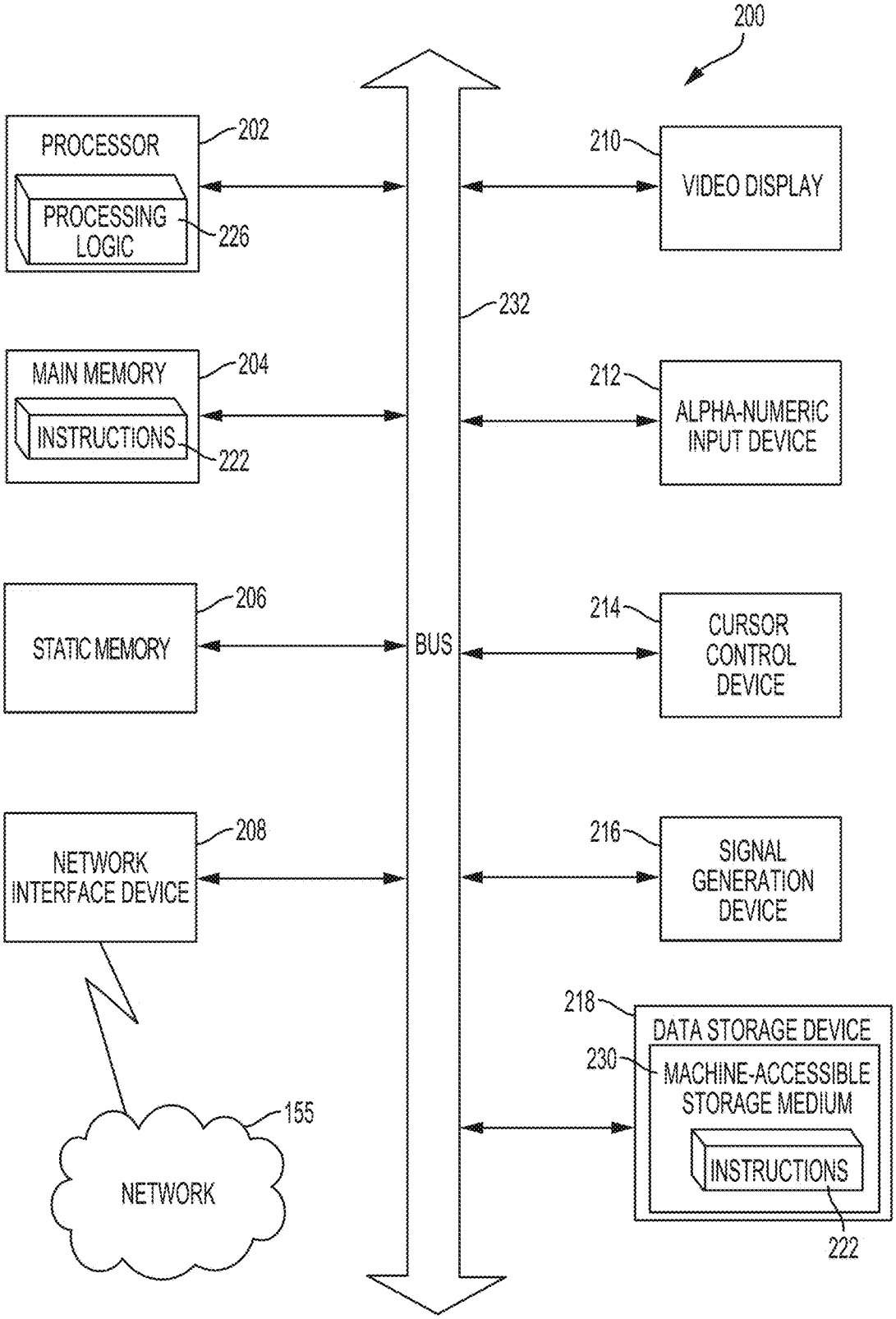

200
PROCESSOR
202
PROCESSING LOGIC
226
MAIN MEMORY
204
INSTRUCTIONS
222
STATIC MEMORY
206
NETWORK INTERFACE DEVICE
208
NETWORK
155
BUS
232
VIDEO DISPLAY
210
ALPHA-NUMERIC INPUT DEVICE
212
CURSOR CONTROL DEVICE
214
SIGNAL GENERATION DEVICE
216
DATA STORAGE DEVICE
218
MACHINE-ACCESSIBLE STORAGE MEDIUM
230
INSTRUCTIONS
222

FIG. 2A

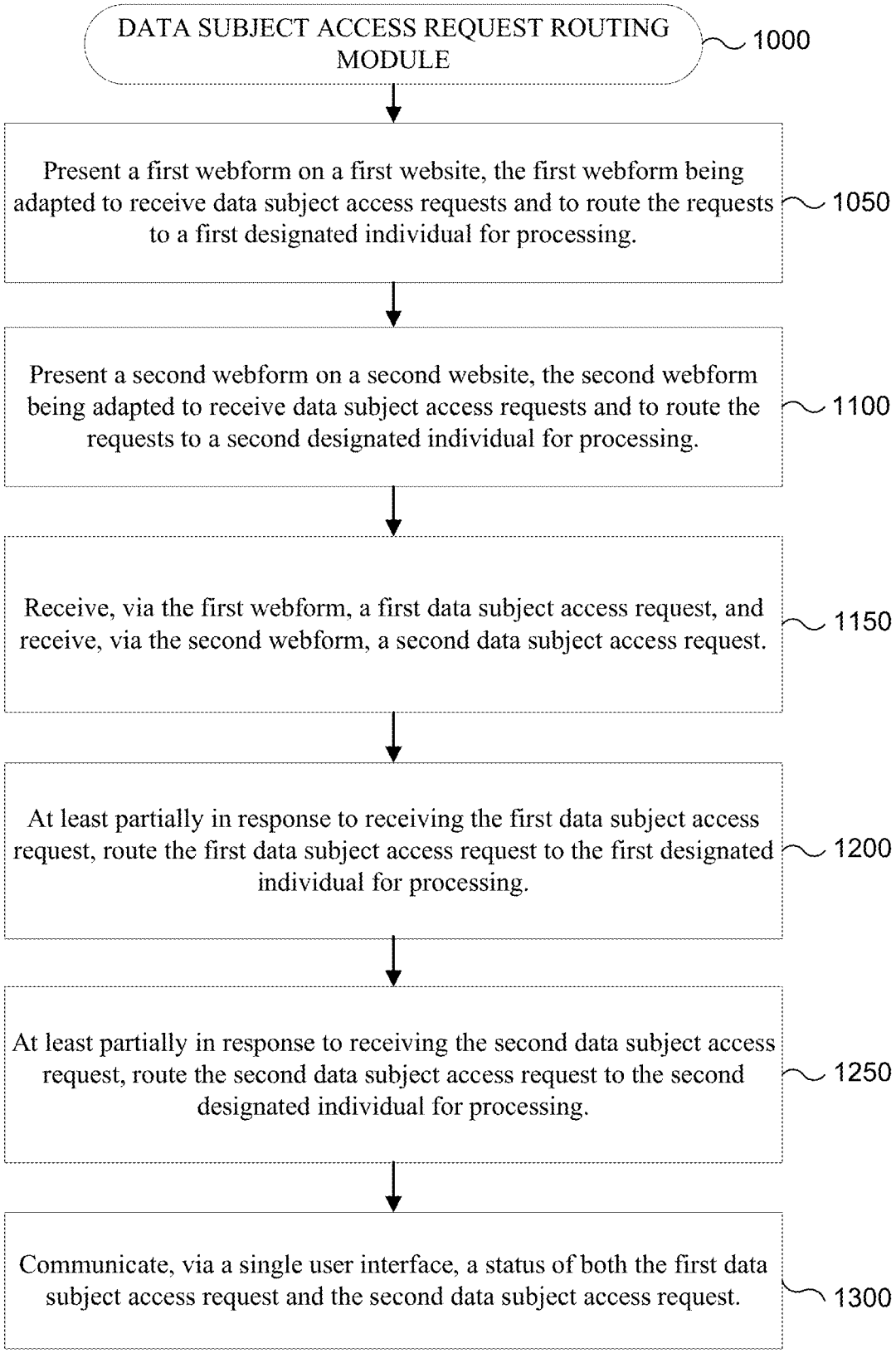

DATA SUBJECT ACCESS REQUEST ROUTING MODULE
1000
Present a first webform on a first website, the first webform being adapted to receive data subject access requests and to route the requests to a first designated individual for processing.
1050
Present a second webform on a second website, the second webform being adapted to receive data subject access requests and to route the requests to a second designated individual for processing.
1100
Receive, via the first webform, a first data subject access request, and receive, via the second webform, a second data subject access request.
1150
At least partially in response to receiving the first data subject access request, route the first data subject access request to the first designated individual for processing.
1200
At least partially in response to receiving the second data subject access request, route the second data subject access request to the second designated individual for processing.
1250
Communicate, via a single user interface, a status of both the first data subject access request and the second data subject access request.
1300

FIG. 2B

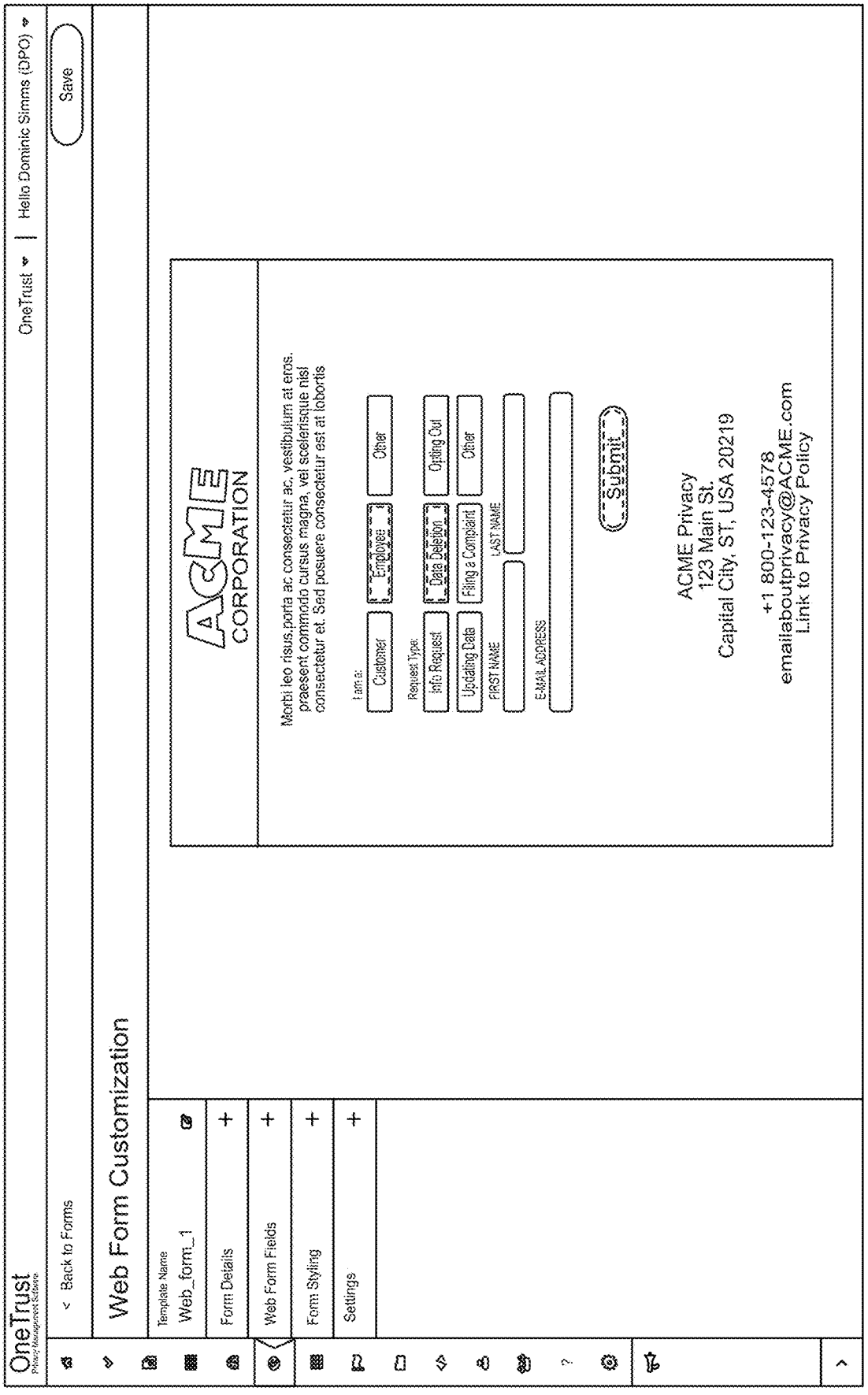

OneTrust
Privacy Management Software
OneTrust | Hello Dominic Simms (DPO)
< Back to Forms
Save
Web Form Customization
Template Name
Web_form_1
Form Details
Web Form Fields
Form Styling
Settings
ACME
CORPORATION
Morbi leo risus,porta ac consectetur ac, vestibulum at eros. praesent commodo cursus magna, vel scelerisque nisl consectetur et. Sed posuere consectetur est at lobortis
I am a:
Customer
Employee
Other
Request Type:
Info Request
Data Deletion
Opting Out
Updating Data
Filing a Complaint
Other
FIRST NAME
LAST NAME
E-MAIL ADDRESS
Submit
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 3

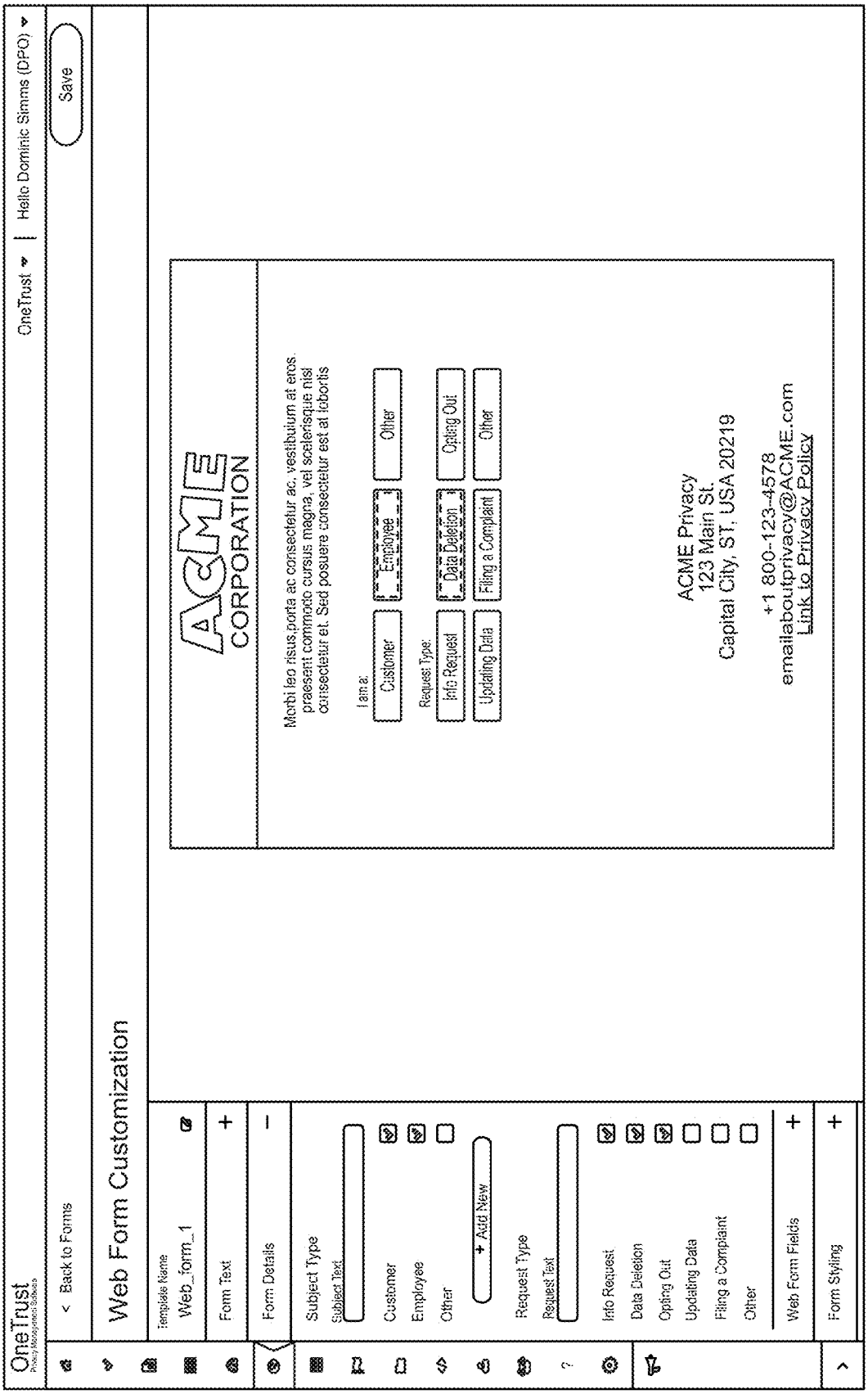

OneTrust
Privacy Management Software
OneTrust
Hello Dominic Simms (DPO)
< Back to Forms
Save
Web Form Customization
Template Name
Web_form_1
Form Text
Form Details
Subject Type
Subject Text
Customer
Employee
Other
+ Add New
Request Type
Request Text
Info Request
Data Deletion
Opting Out
Updating Data
Filing a Complaint
Other
Web Form Fields
Form Styling
ACME
CORPORATION
Morbi leo risus,porta ac consectetur ac, vestibulum at eros. praesent commodo cursus magna, vel scelerisque nisl consectetur et. Sed posuere consectetur est at lobortis
I am a:
Customer
Employee
Other
Request Type:
Info Request
Data Deletion
Opting Out
Updating Data
Filing a Complaint
Other
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 4

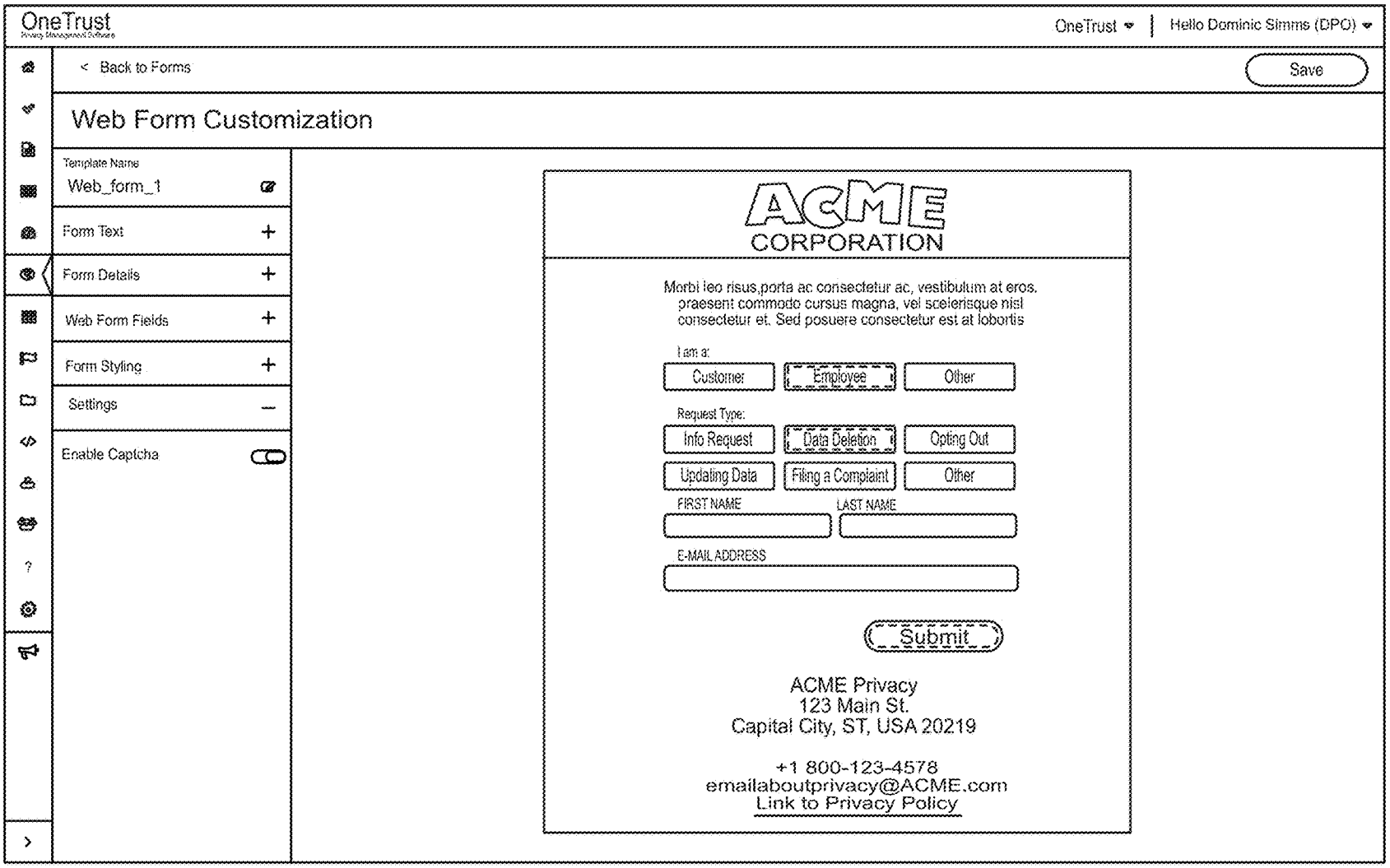

OneTrust
Privacy Management Software
OneTrust
Hello Dominic Simms (DPO)
< Back to Forms
Save
Web Form Customization
Template Name
Web_form_1
Form Text
Form Details
Web Form Fields
Form Styling
Settings
Enable Captcha
ACME
CORPORATION
Morbi leo risus,porta ac consectetur ac, vestibulum at eros. praesent commodo cursus magna, vel scelerisque nisl consectetur et. Sed posuere consectetur est at lobortis
I am a:
Customer
Employee
Other
Request Type:
Info Request
Data Deletion
Opting Out
Updating Data
Filing a Complaint
Other
FIRST NAME
LAST NAME
E-MAIL ADDRESS
Submit
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 5

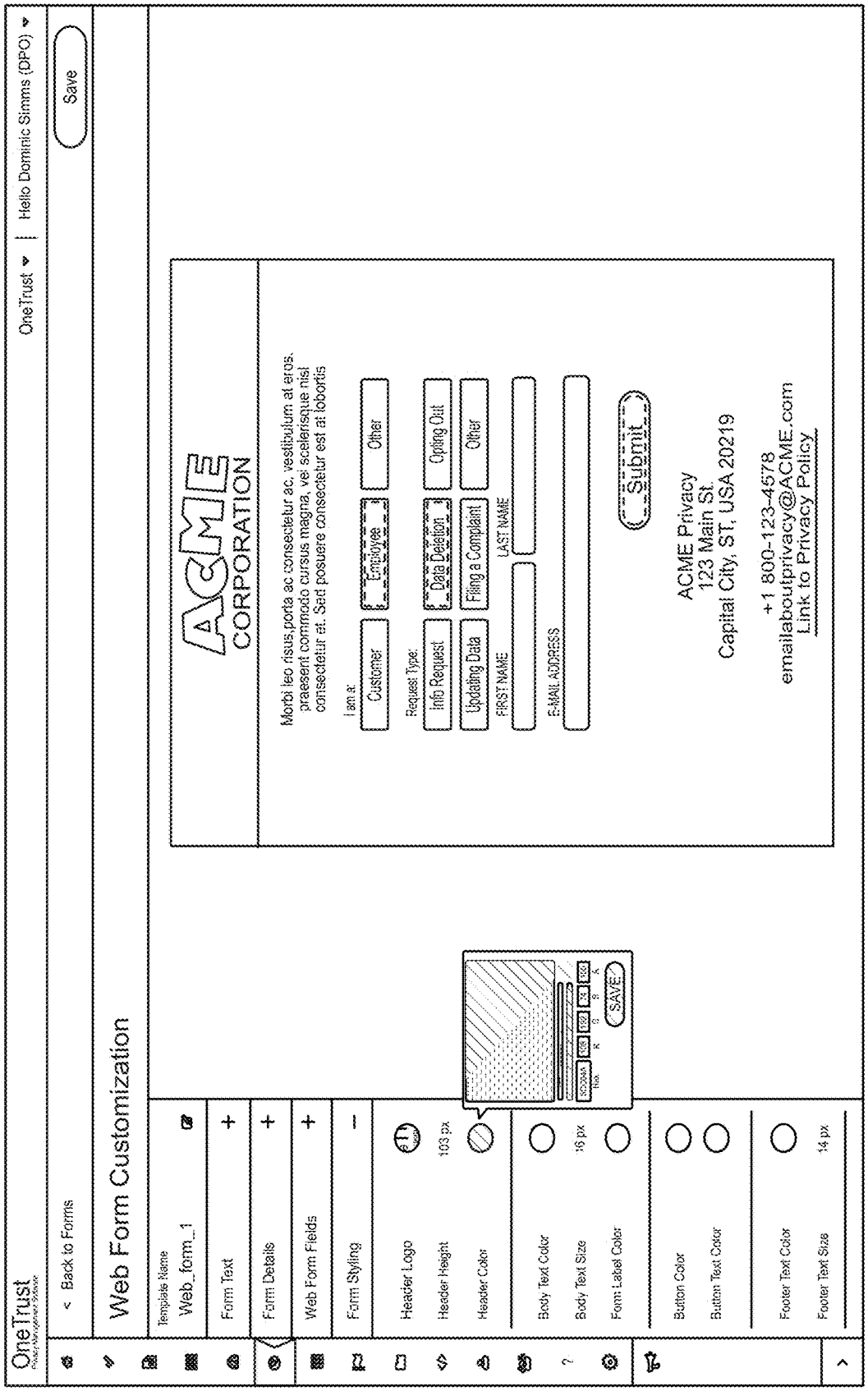

OneTrust
OneTrust
Hello Dominic Simms (DPO)
< Back to Forms
Save
Web Form Customization
Template Name
Web_form_1
Form Text
Form Details
Web Form Fields
Form Styling
Header Logo
Header Height
103 px
Header Color
Body Text Color
Body Text Size
16 px
Form Label Color
Button Color
Button Text Color
Footer Text Color
Footer Text Size
14 px
SAVE
ACME
CORPORATION
Morbi leo risus,porta ac consectetur ac, vestibulum at eros. praesent commodo cursus magna, vel scelerisque nisl consectetur at. Sed posuere consectetur est at lobortis
I am a:
Customer
Employee
Other
Request Type:
Info Request
Data Deletion
Opting Out
Updating Data
Filing a Complaint
Other
FIRST NAME
LAST NAME
E-MAIL ADDRESS
Submit
ACME Privacy
123 Main St
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 6

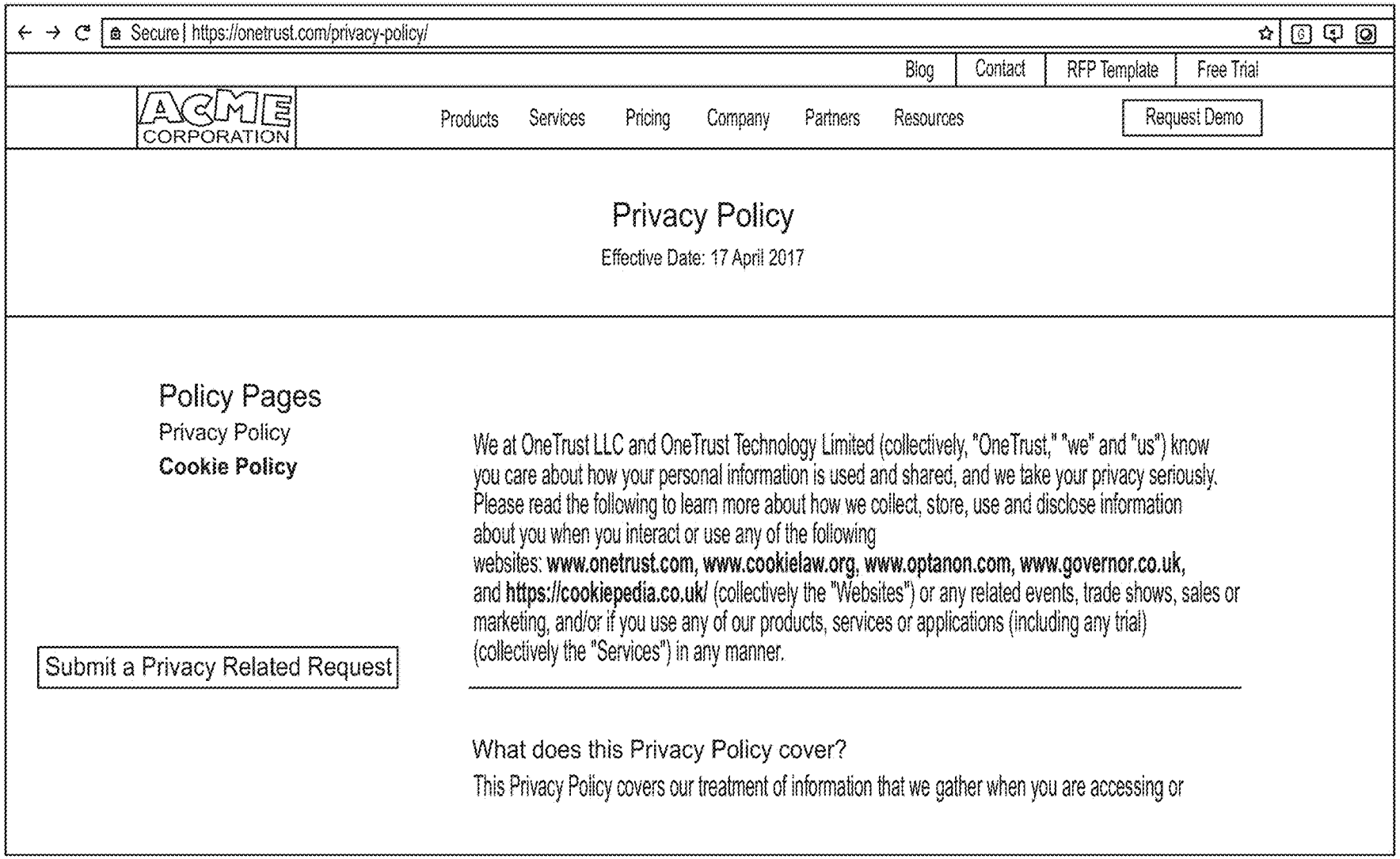

Secure | https://onetrust.com/privacy-policy/
Blog
Contact
RFP Template
Free Trial
ACME CORPORATION
Products
Services
Pricing
Company
Partners
Resources
Request Demo
Privacy Policy
Effective Date: 17 April 2017
Policy Pages
Privacy Policy
Cookie Policy
Submit a Privacy Related Request
We at OneTrust LLC and OneTrust Technology Limited (collectively, "OneTrust," "we" and "us") know you care about how your personal information is used and shared, and we take your privacy seriously. Please read the following to learn more about how we collect, store, use and disclose information about you when you interact or use any of the following websites: www.onetrust.com, www.cookielaw.org, www.optanon.com, www.governor.co.uk, and https://cookiepedia.co.uk/ (collectively the "Websites") or any related events, trade shows, sales or marketing, and/or if you use any of our products, services or applications (including any trial) (collectively the "Services") in any manner.
What does this Privacy Policy cover?
This Privacy Policy covers our treatment of information that we gather when you are accessing or

FIG. 7

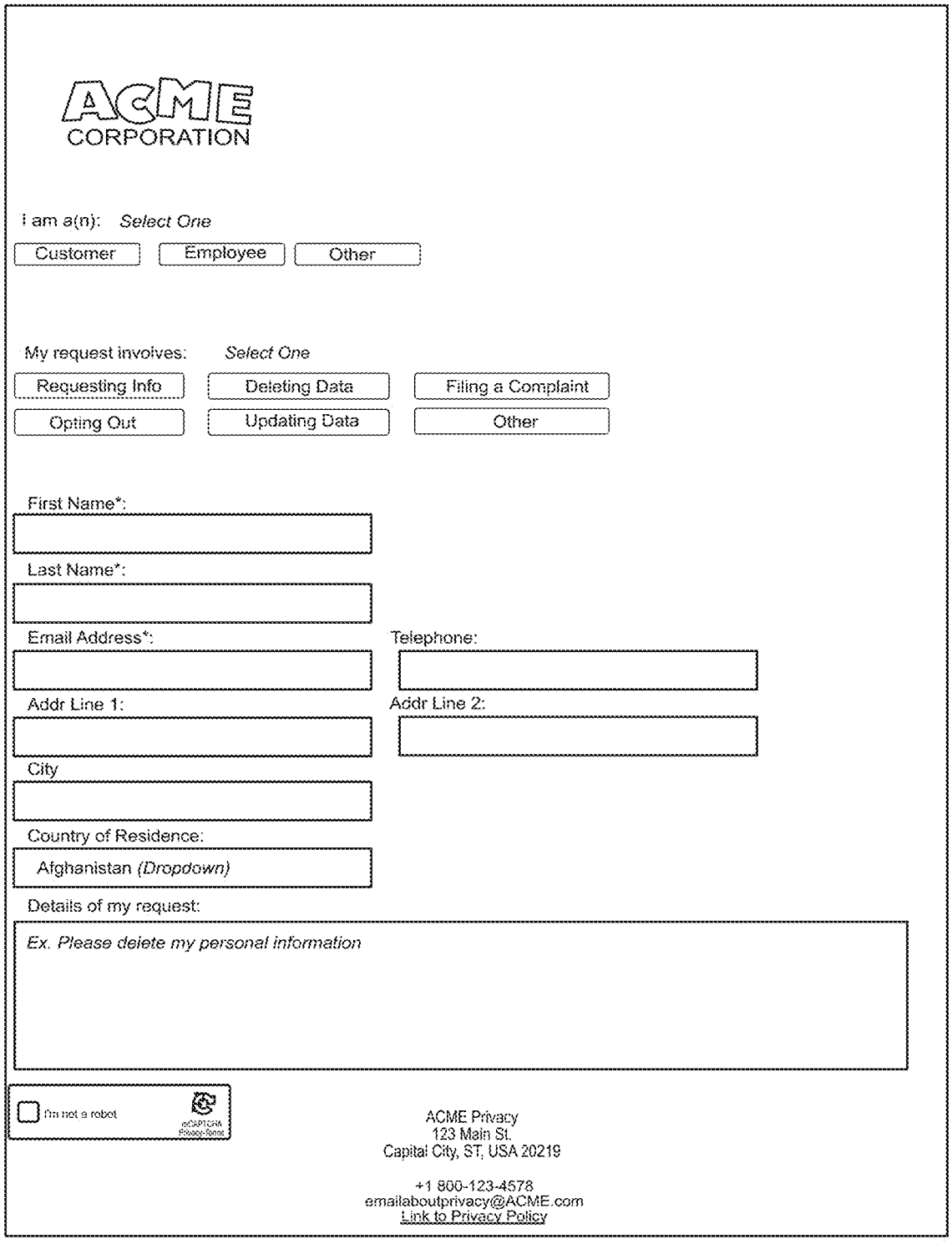

ACME
CORPORATION
I am a(n): Select One
Customer
Employee
Other
My request involves: Select One
Requesting Info
Deleting Data
Filing a Complaint
Opting Out
Updating Data
Other
First Name*:
Last Name*:
Email Address*:
Telephone:
Addr Line 1:
Addr Line 2:
City
Country of Residence:
Afghanistan (Dropdown)
Details of my request:
Ex. Please delete my personal information
I'm not a robot
reCAPTCHA
Privacy - Terms
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 8

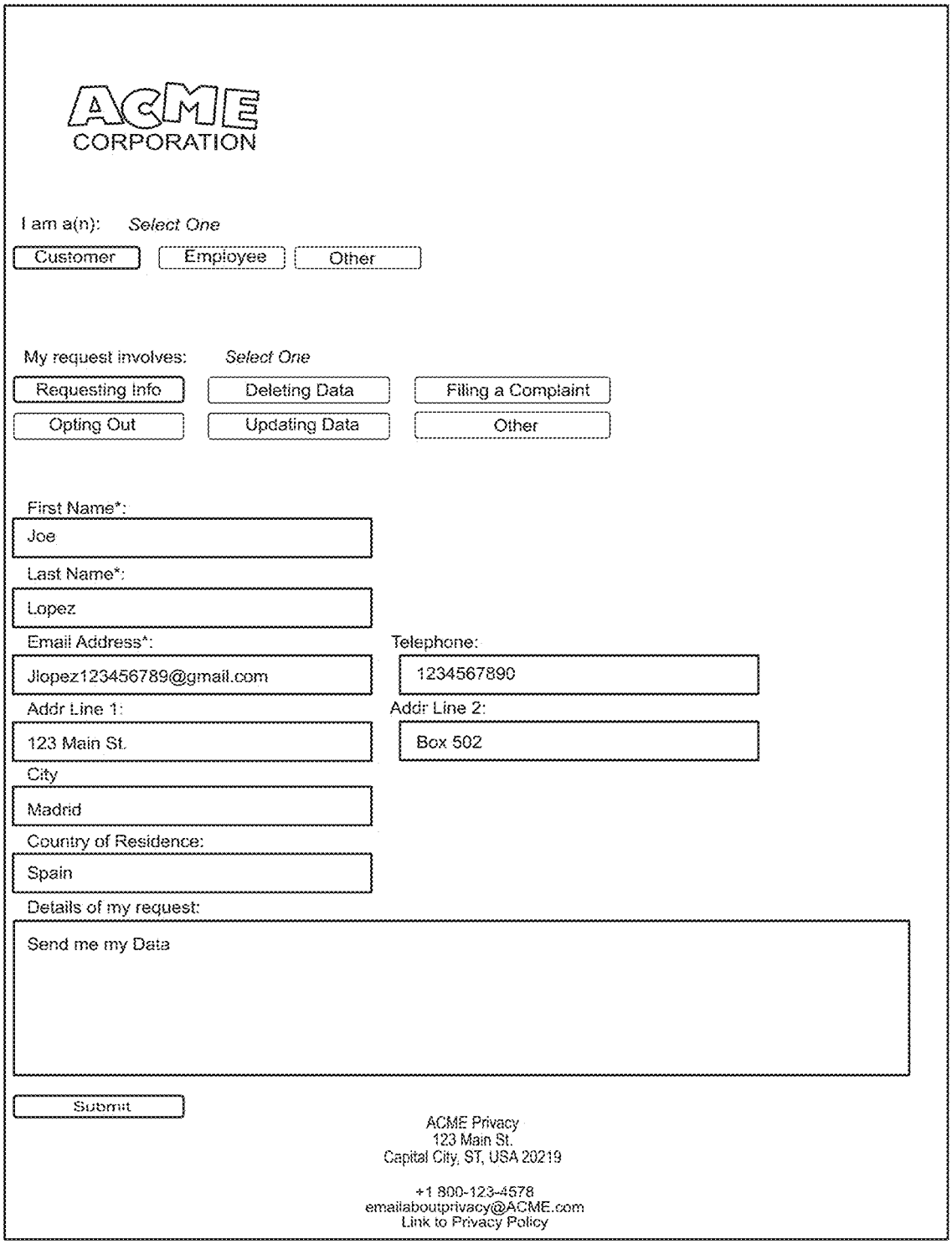

ACME
CORPORATION
I am a(n): Select One
Customer
Employee
Other
My request involves: Select One
Requesting Info
Deleting Data
Filing a Complaint
Opting Out
Updating Data
Other
First Name*:
Joe
Last Name*:
Lopez
Email Address*:
Jlopez123456789@gmail.com
Telephone:
1234567890
Addr Line 1:
123 Main St.
Addr Line 2:
Box 502
City
Madrid
Country of Residence:
Spain
Details of my request:
Send me my Data
Submit
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 9

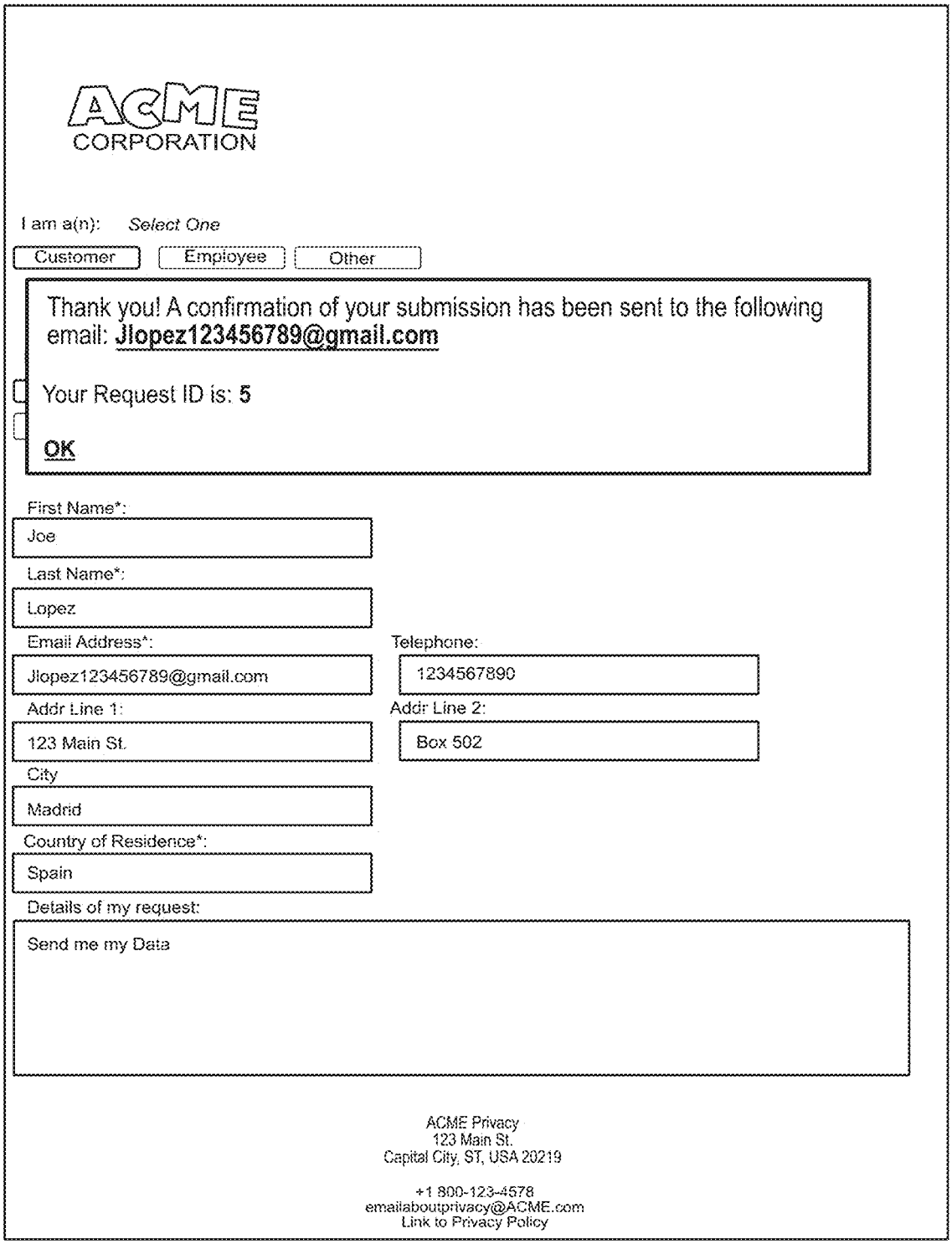

ACME
CORPORATION
I am a(n): Select One
Customer
Employee
Other
Thank you! A confirmation of your submission has been sent to the following email: Jlopez123456789@gmail.com
Your Request ID is: 5
OK
First Name*:
Joe
Last Name*:
Lopez
Email Address*:
Jlopez123456789@gmail.com
Telephone:
1234567890
Addr Line 1:
123 Main St.
Addr Line 2:
Box 502
City
Madrid
Country of Residence*:
Spain
Details of my request:
Send me my Data
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 10

From: OneTrust Privacy Officer
Sent: Sunday, February 19, 2017 9:27 PM EST
To: Joe Lopez <jlopez123456789@gmail.com>
BCc: Amelia Davis <adavis09876@ACME.com>
Subject: *Your ACME Privacy Request is being processed*

ACME CORPORATION

Data Request

Thank you for your submission! Here are the details of your request:

Request ID: 5
Date Submitted: 2/21/2017 10:35AM EST
I am a(n): Customer
My request involves: Opting Out
First Name*: Joe
Last Name*: Lopez
Email Address*: Jlopez123456789@gmail.com
Telephone: XXXXXX986
Addr Line 1: XXXXXXXXXX
Addr Line 2: XXXXXXXXXX
City: XXXXXXXXXX
Count of Residence*: XXXXXXXXXX
Details of my request:
Send me my Data

If you have any questions regarding your submission, please contact *Amelia Davis* via email or phone:
adavis09876@ACME.com
+00 123 123 9980

ACME Privacy
123 Main St.
Capital City, ST, USA 20219

+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 11

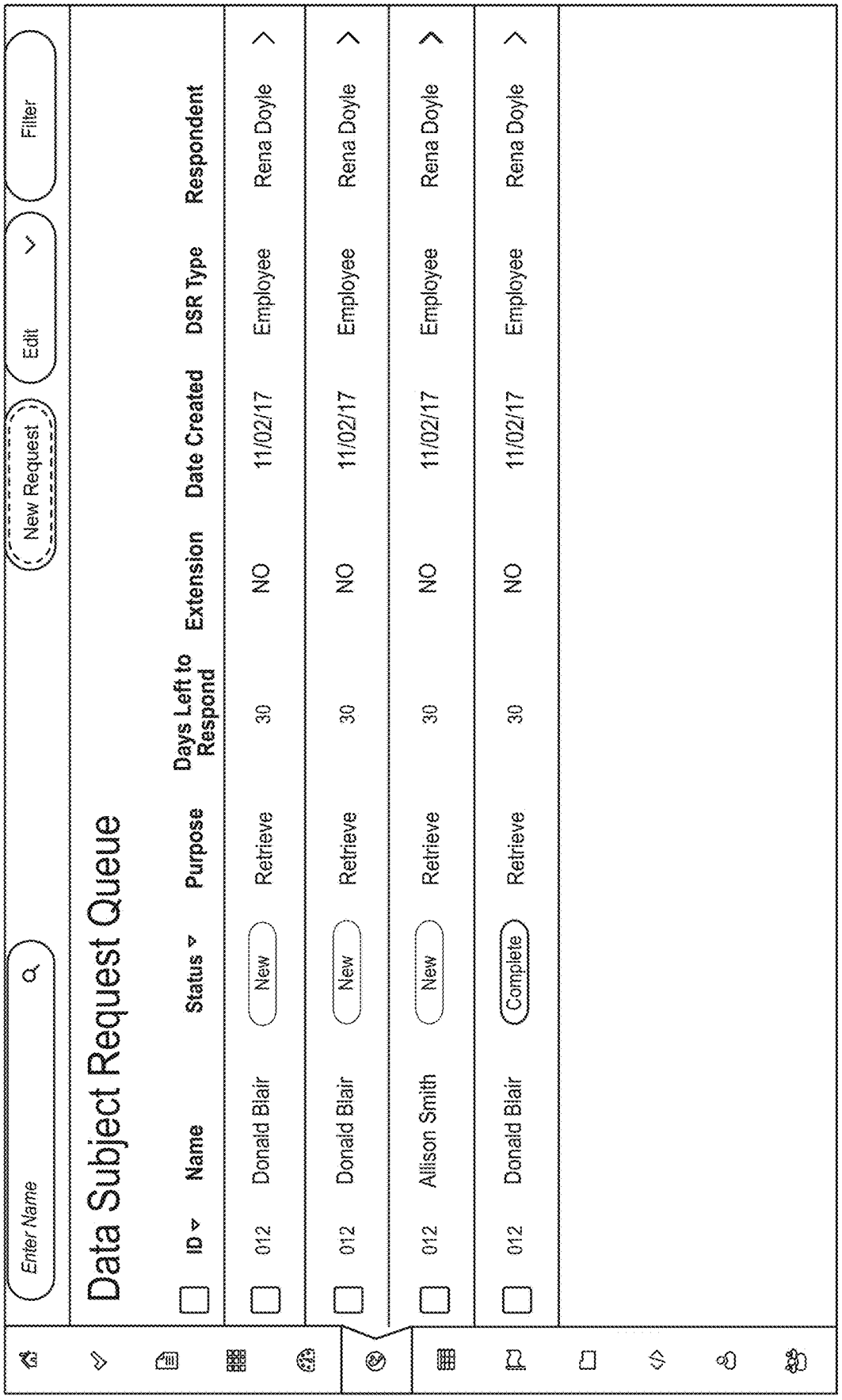

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Allison Smith New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 12

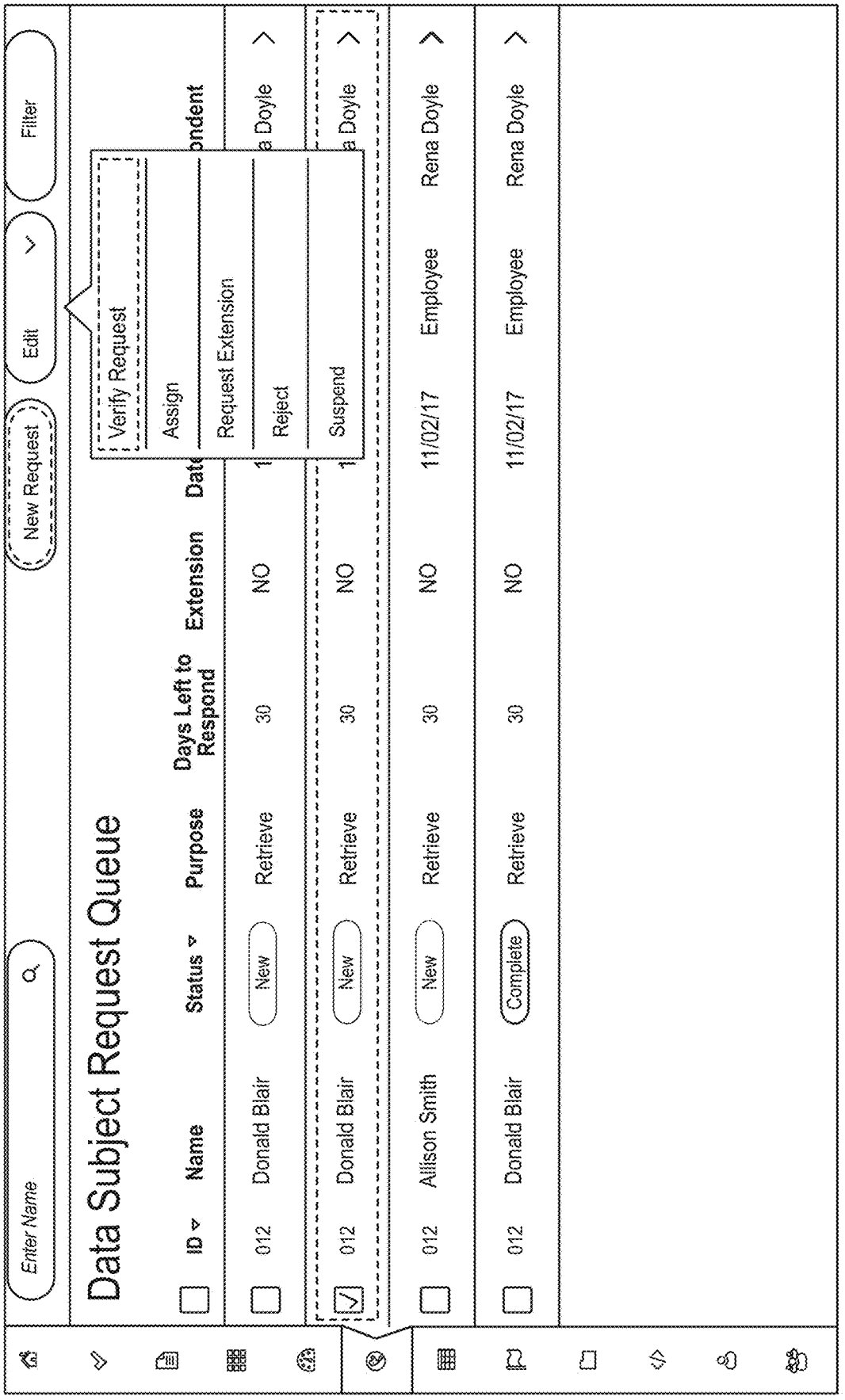

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Dat
012 Donald Blair New Retrieve 30 NO
012 Donald Blair New Retrieve 30 NO
012 Allison Smith New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle
Verify Request
Assign
Request Extension
Reject
Suspend
ndent
a Doyle
a Doyle

FIG. 13

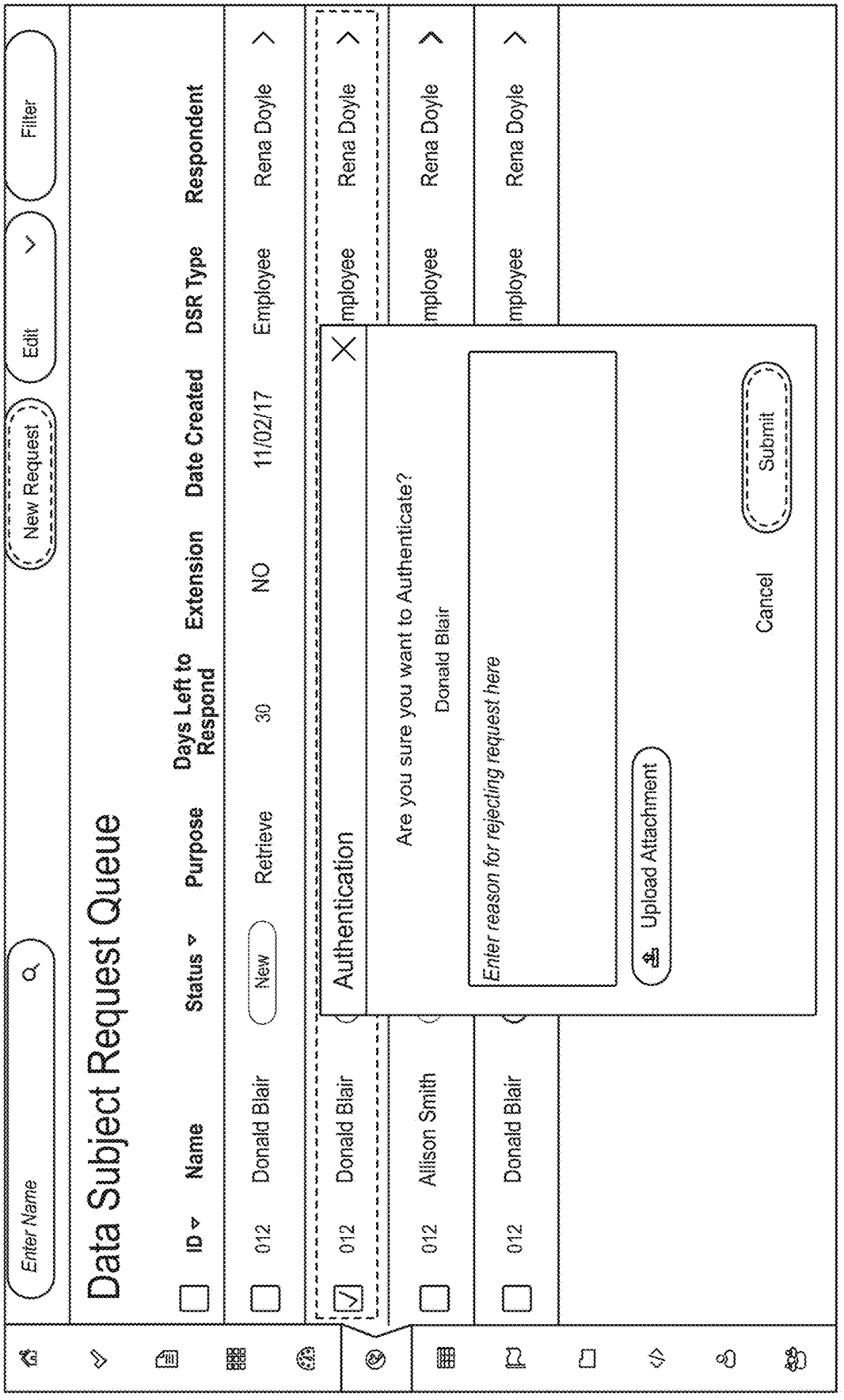

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Authentication
012 Allison Smith
012 Donald Blair
Are you sure you want to Authenticate?
Donald Blair
Enter reason for rejecting request here
Upload Attachment
Cancel
Submit

FIG. 14

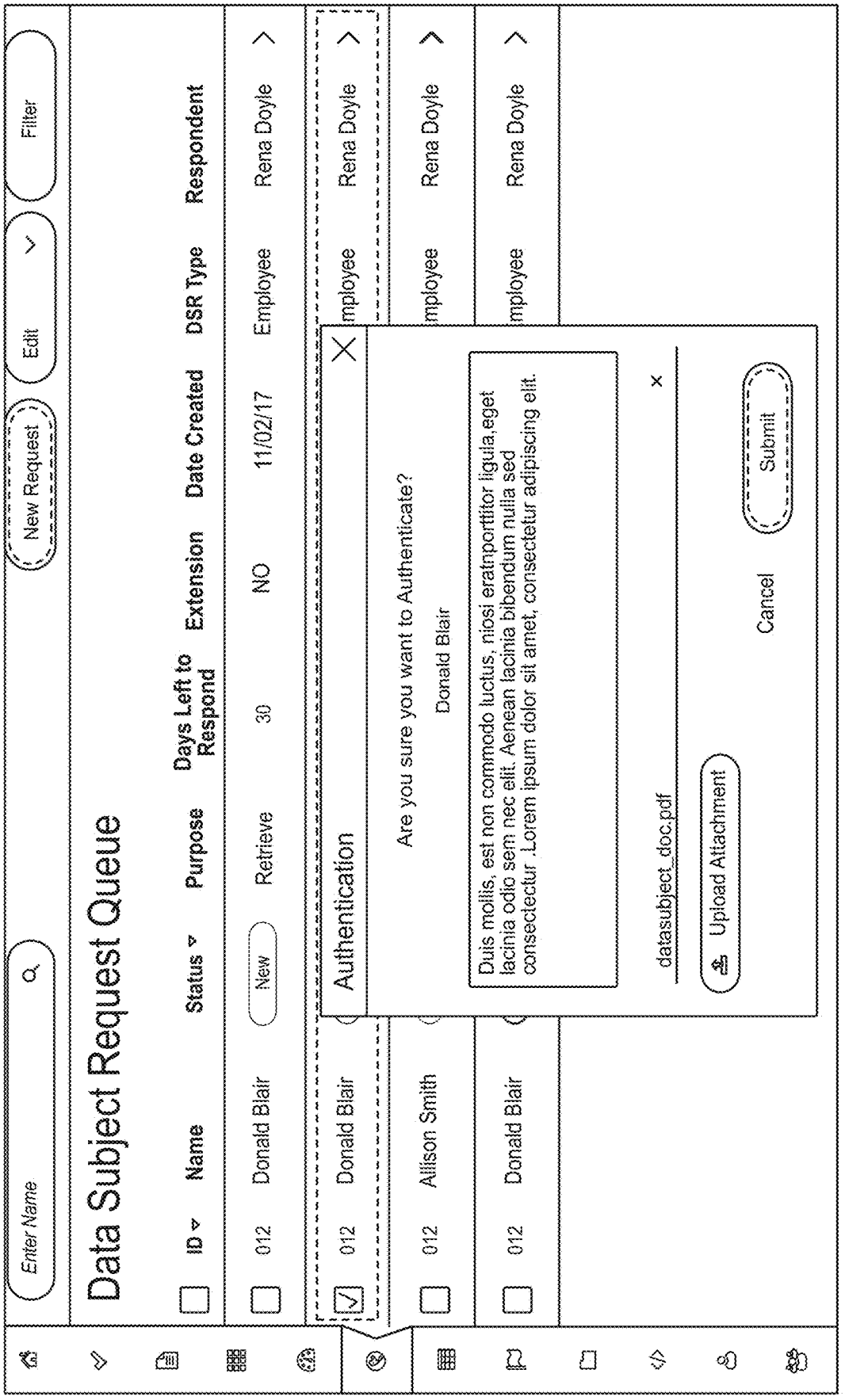

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Authentication
Are you sure you want to Authenticate?
Donald Blair
Duis mollis, est non commodo luctus, nisi eratnporttitor ligula,eget lacinia odio sem nec elit. Aenean lacinia bibendum nulla sed consectectur .Lorem ipsum dolor sit amet, consectetur adipiscing elit.
datasubject_doc.pdf
Upload Attachment
Cancel
Submit
012 Allison Smith
012 Donald Blair

FIG. 15

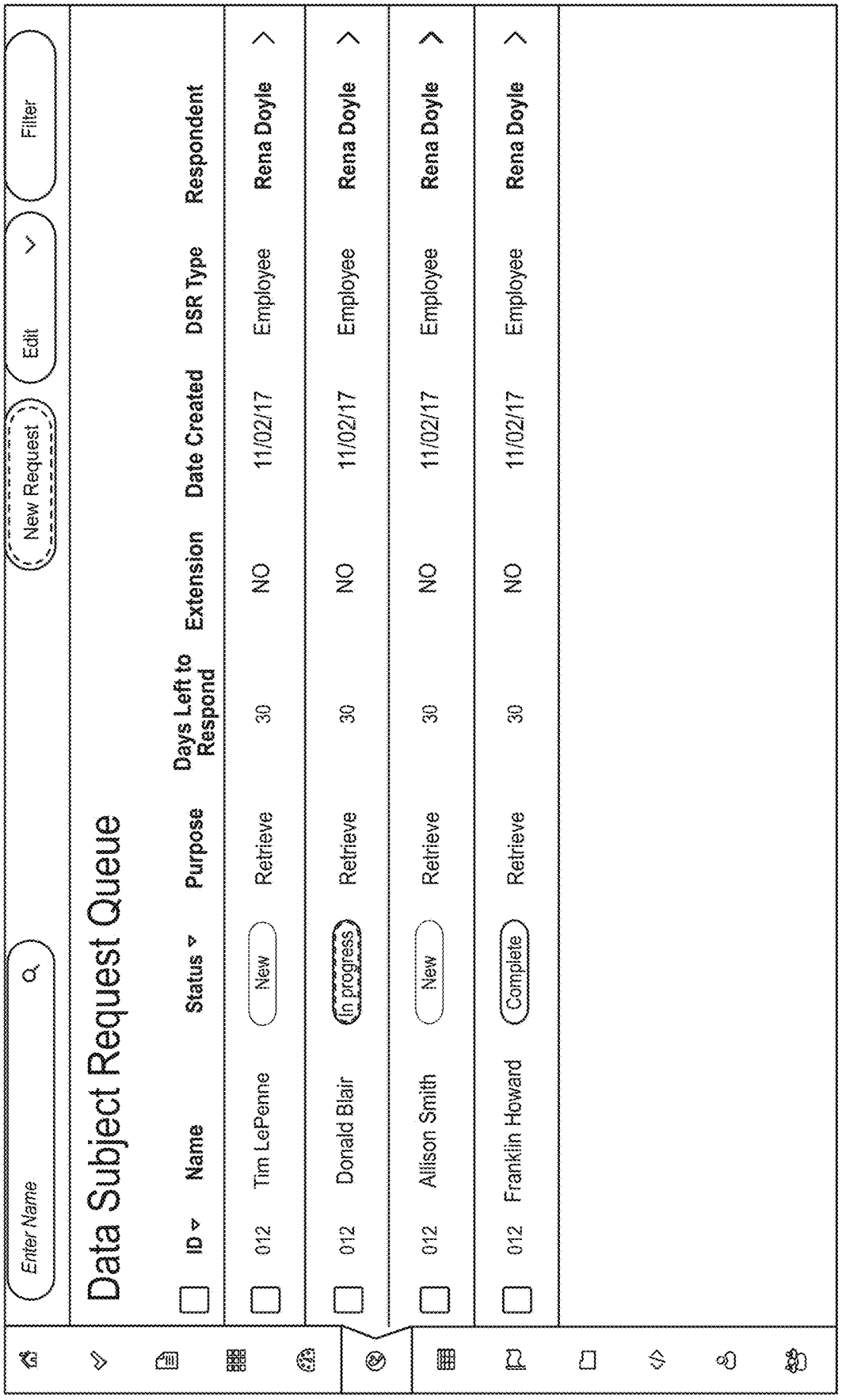

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012
Tim LePenne
New
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Donald Blair
In progress
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Allison Smith
New
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Franklin Howard
Complete
Retrieve
30
NO
11/02/17
Employee
Rena Doyle

FIG. 16

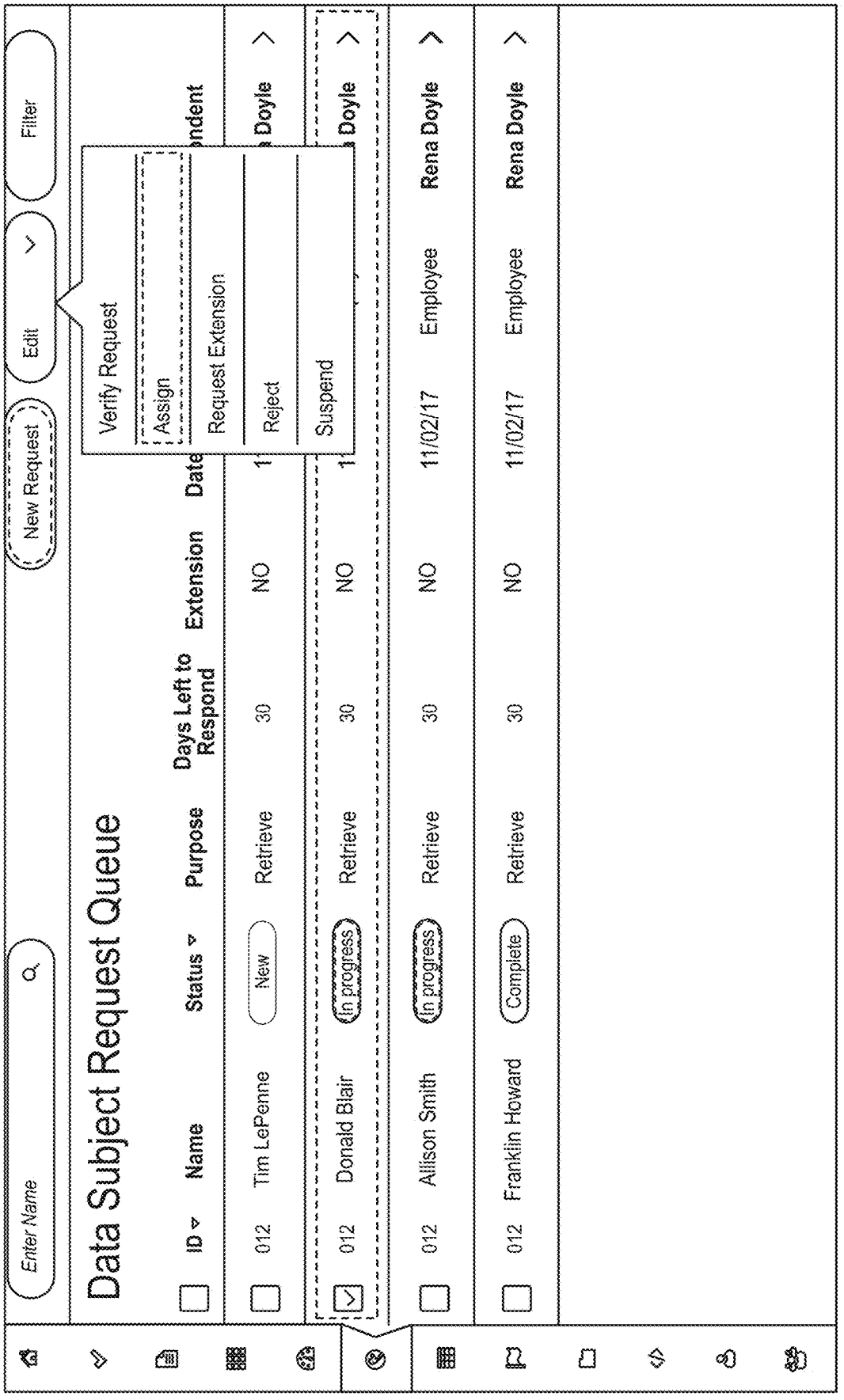

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date
Verify Request
Assign
Request Extension
Reject
Suspend
012 Tim LePenne New Retrieve 30 NO 1 Doyle
012 Donald Blair In progress Retrieve 30 NO 1 Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 17

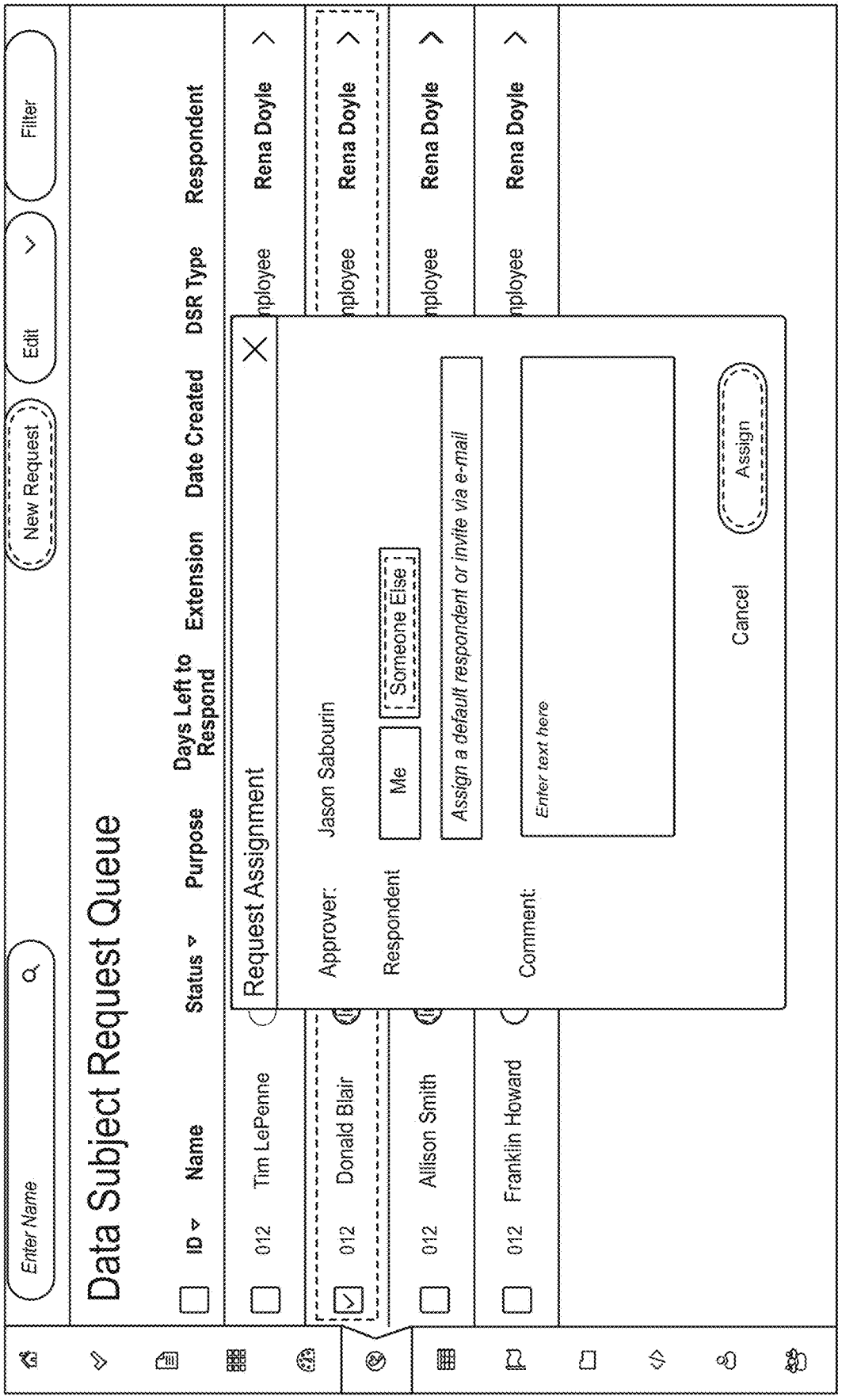

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Tim LePenne
012 Donald Blair
012 Allison Smith
012 Franklin Howard
Rena Doyle
Request Assignment
Approver:
Jason Sabourin
Respondent:
Me
Someone Else
Assign a default respondent or invite via e-mail
Comment:
Enter text here
Cancel
Assign

FIG. 18

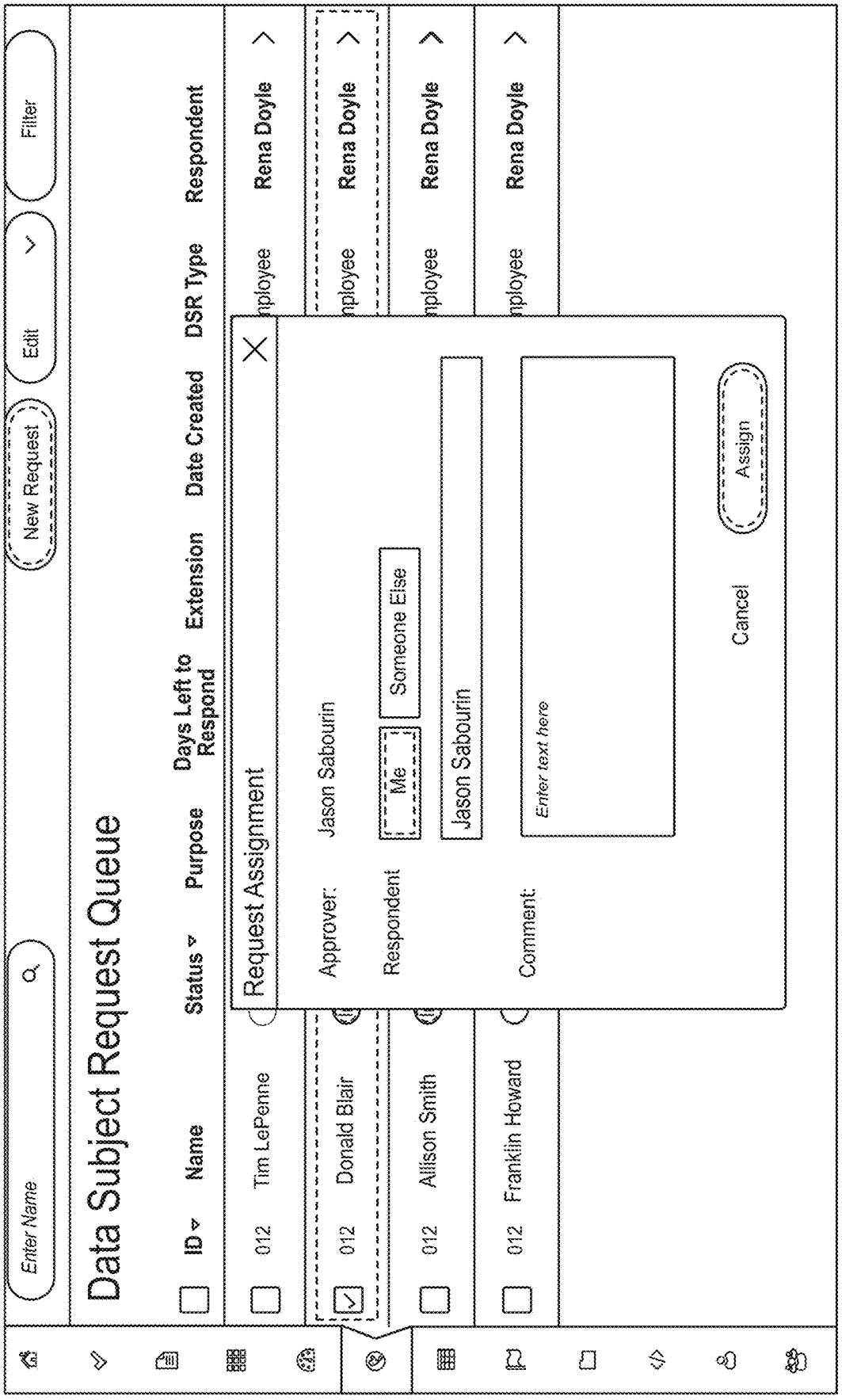

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Tim LePenne
012 Donald Blair
012 Allison Smith
012 Franklin Howard
Rena Doyle
Request Assignment
Approver:
Jason Sabourin
Respondent
Me
Someone Else
Jason Sabourin
Comment:
Enter text here
Cancel
Assign

FIG. 19

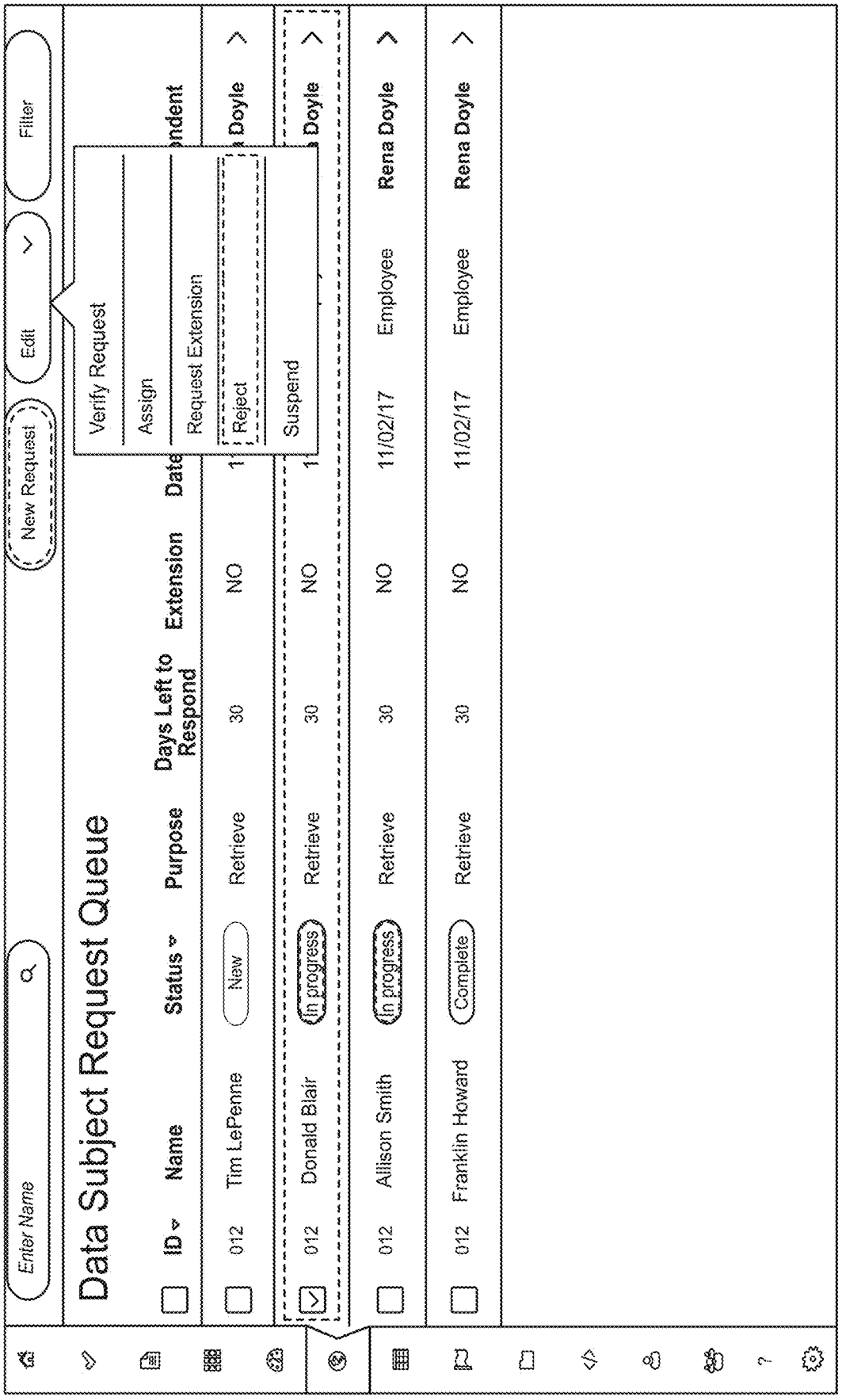

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date
Verify Request
Assign
Request Extension
Reject
Suspend
012 Tim LePenne New Retrieve 30 NO 11 Doyle
012 Donald Blair In progress Retrieve 30 NO 11 Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 20

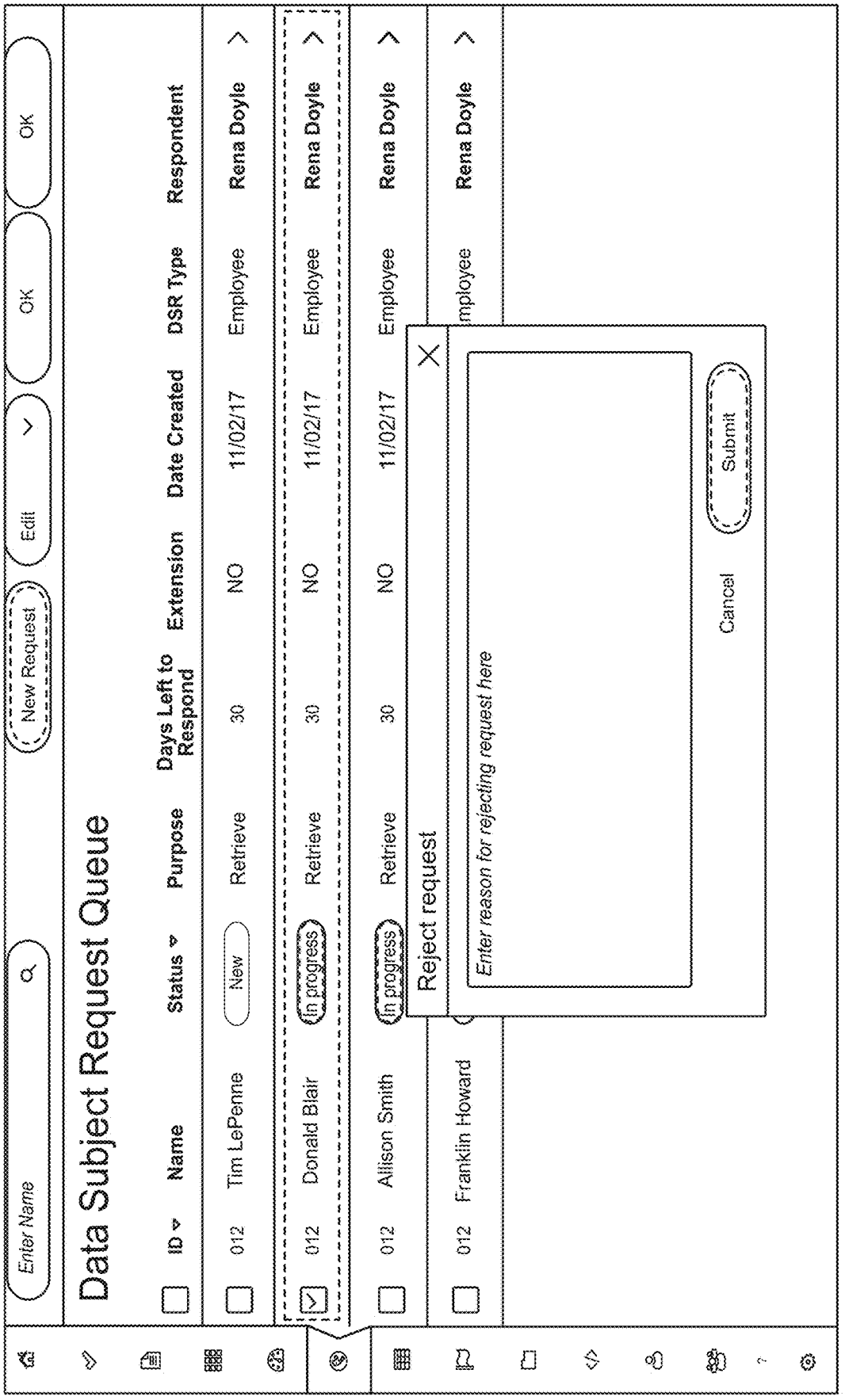

Enter Name
New Request
Edit
OK
OK
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012
Tim LePenne
New
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Donald Blair
In progress
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Allison Smith
In progress
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Franklin Howard
Rena Doyle
Reject request
Enter reason for rejecting request here
Cancel
Submit

FIG. 21

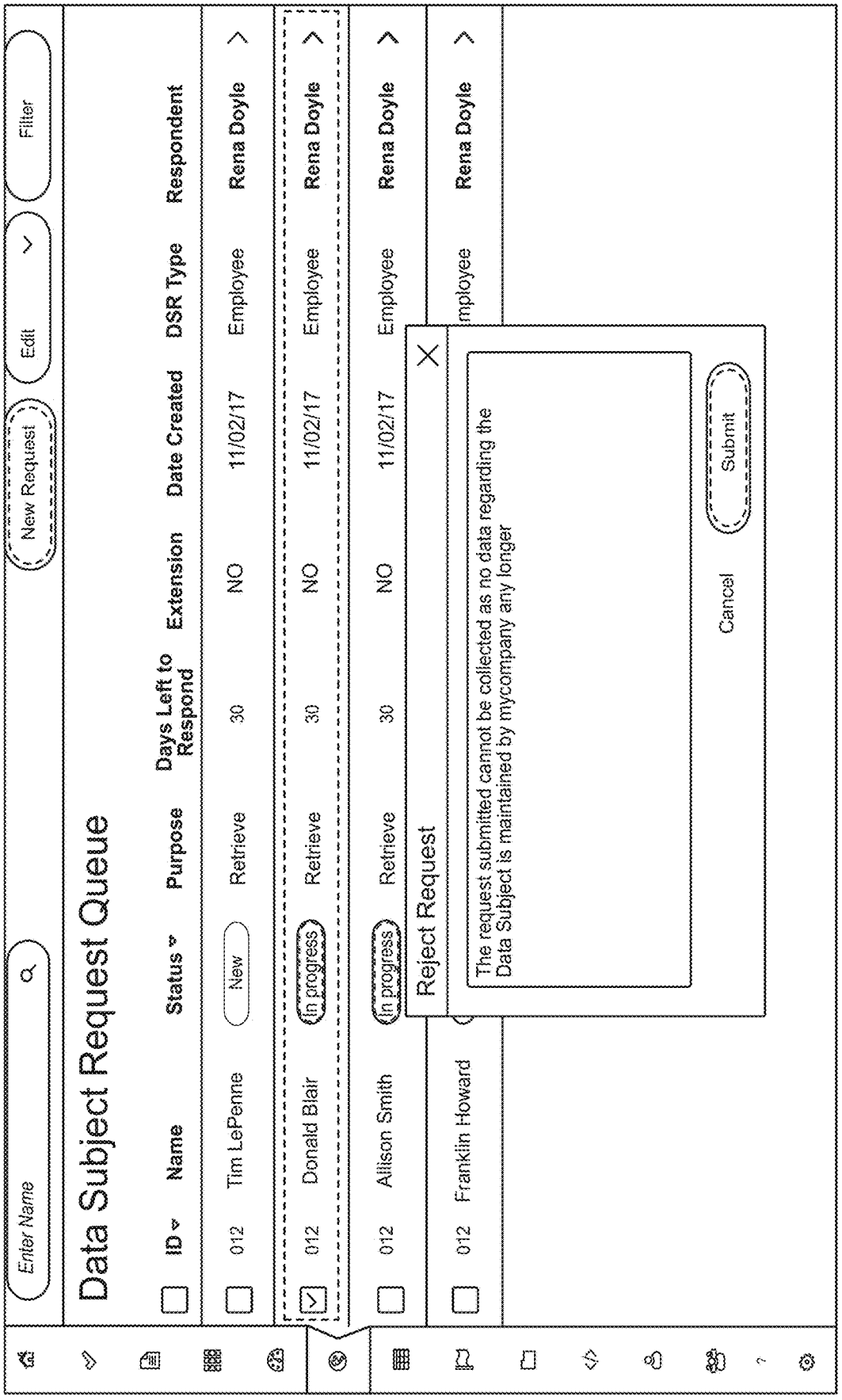

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Tim LePenne New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Retrieve 30 NO 11/02/17 Employee Rena Doyle
Reject Request
The request submitted cannot be collected as no data regarding the Data Subject is maintained by mycompany any longer
Cancel
Submit

FIG. 22

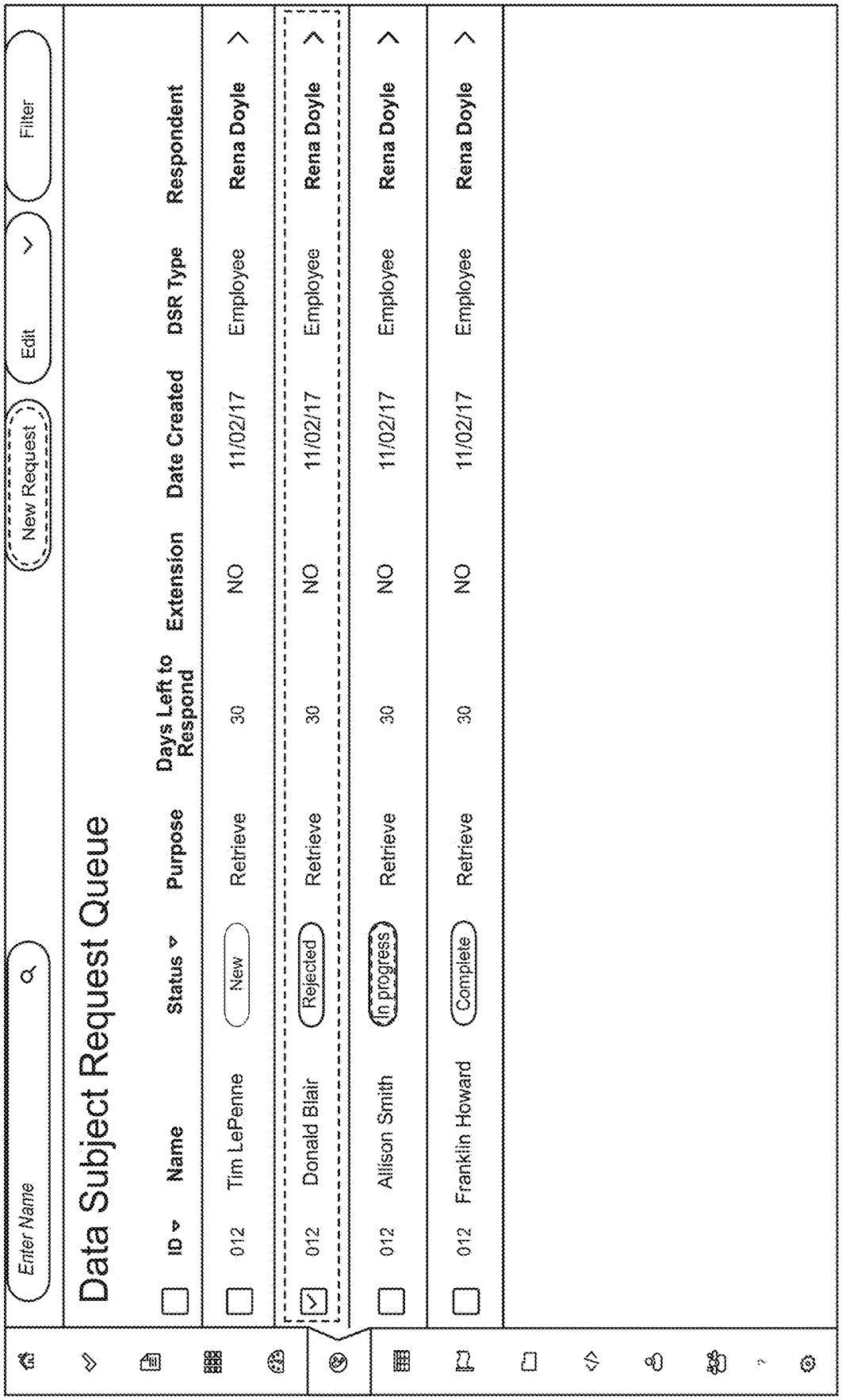

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012
Tim LePenne
New
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Donald Blair
Rejected
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Allison Smith
In progress
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Franklin Howard
Complete
Retrieve
30
NO
11/02/17
Employee
Rena Doyle

FIG. 23

From: OneTrust Privacy Officer
Sent: Sunday, February 19, 2017 9:27 PM EST
To: Allison Smith <asmith123456789@gmail.com>
Bcc: Amelia Davis <adavis09876@ACME.com>
Subject: *Your ACME Privacy Request is being Completed*

ACME CORPORATION

Data Response

Dear Allison,

The request submitted cannot be collected as no data regarding the Data Subject is maintained by *mycompany* any longer

Here are the details of your request:

Request ID: 5
Date Submitted: 2/21/2017 10:35AM EST
I am a(n): Employee
My request involves: Restrict
First Name*: Allison
Last Name*: Smith
Email Address*: asmith123456789@gmail.com
Telephone: XXXXXXXXX
Addr Line 1: XXXXXXXXXX
Addr Line 2: XXXXXXXXXX
City: XXXXXXXXXX
Count of Residence*: XXXXXXXXXX
Details of my request:
Restrict my Data

If you have any questions regarding your submission, please contact *Amelia Davis* via email or phone:
adavis09876@ACME.com
+00 123 123 9980

ACME Privacy
123 Main St.
Capital City, ST, USA 20219

+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 24

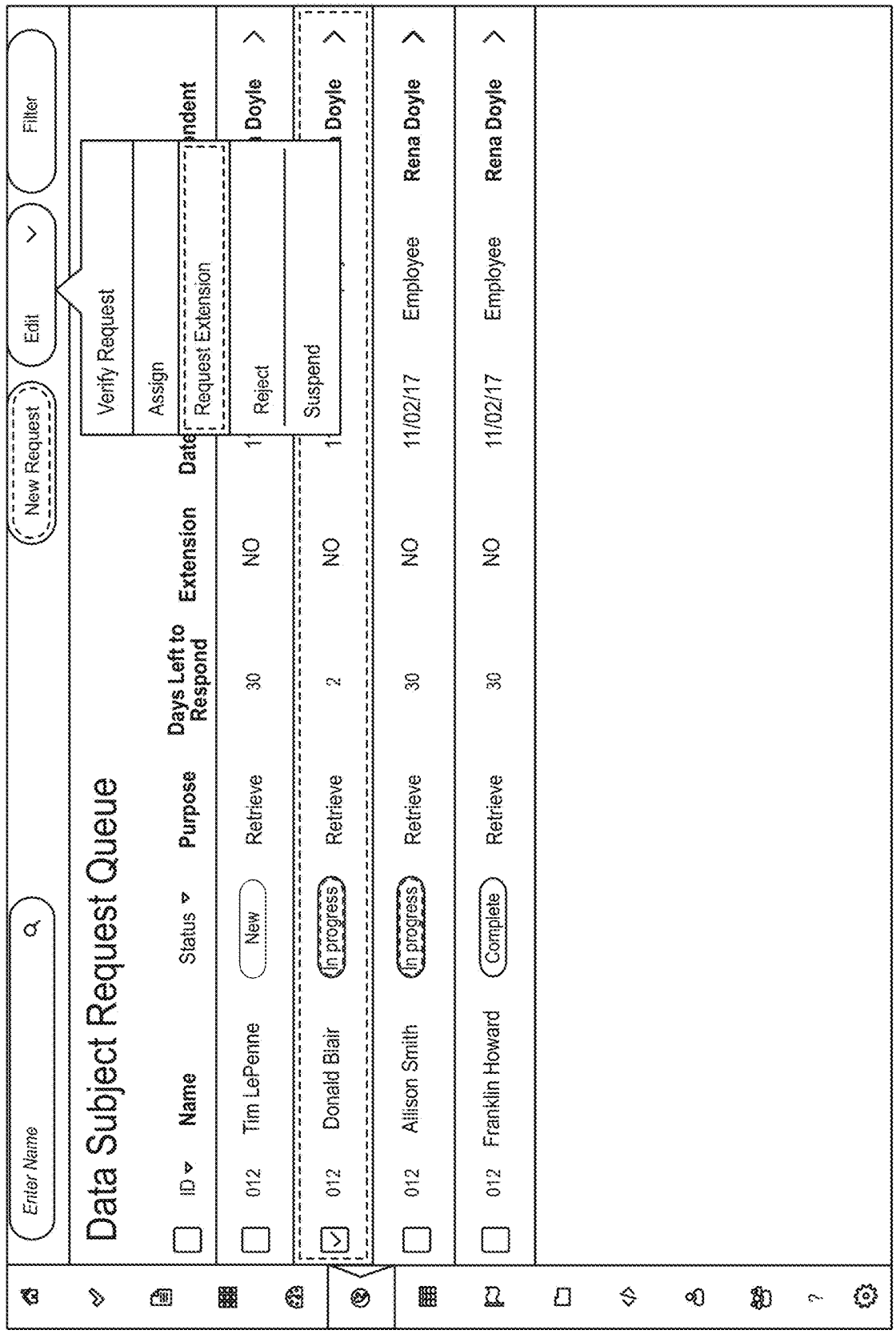

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
Verify Request
Assign
Request Extension
Reject
Suspend
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date
012 Tim LePenne New Retrieve 30 NO 11 Doyle
012 Donald Blair In progress Retrieve 2 NO 11 Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 25

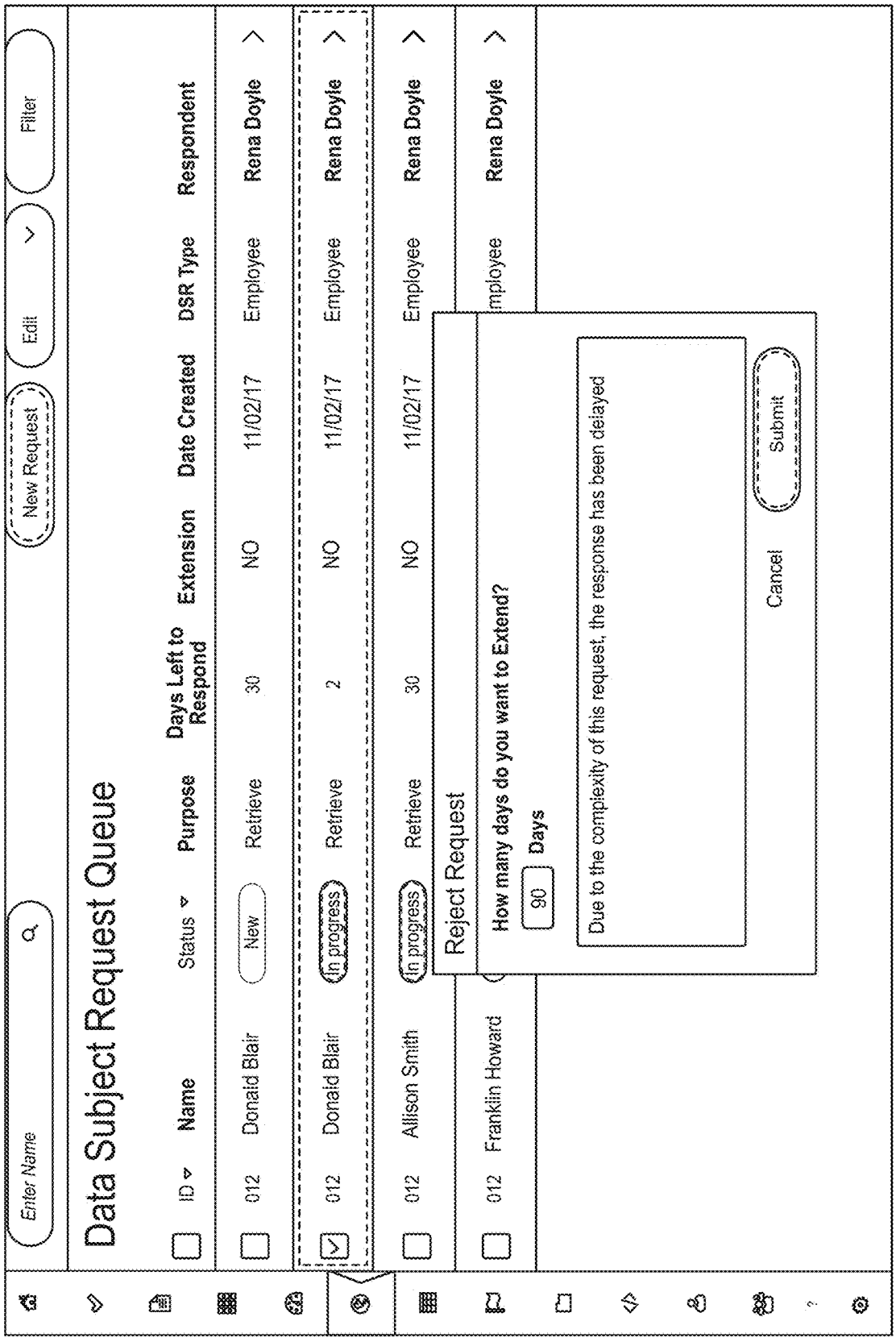

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair In progress Retrieve 2 NO 11/02/17 Employee Rena Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Retrieve 30 NO 11/02/17 Employee Rena Doyle
Reject Request
How many days do you want to Extend?
90
Days
Due to the complexity of this request, the response has been delayed
Cancel
Submit

FIG. 26

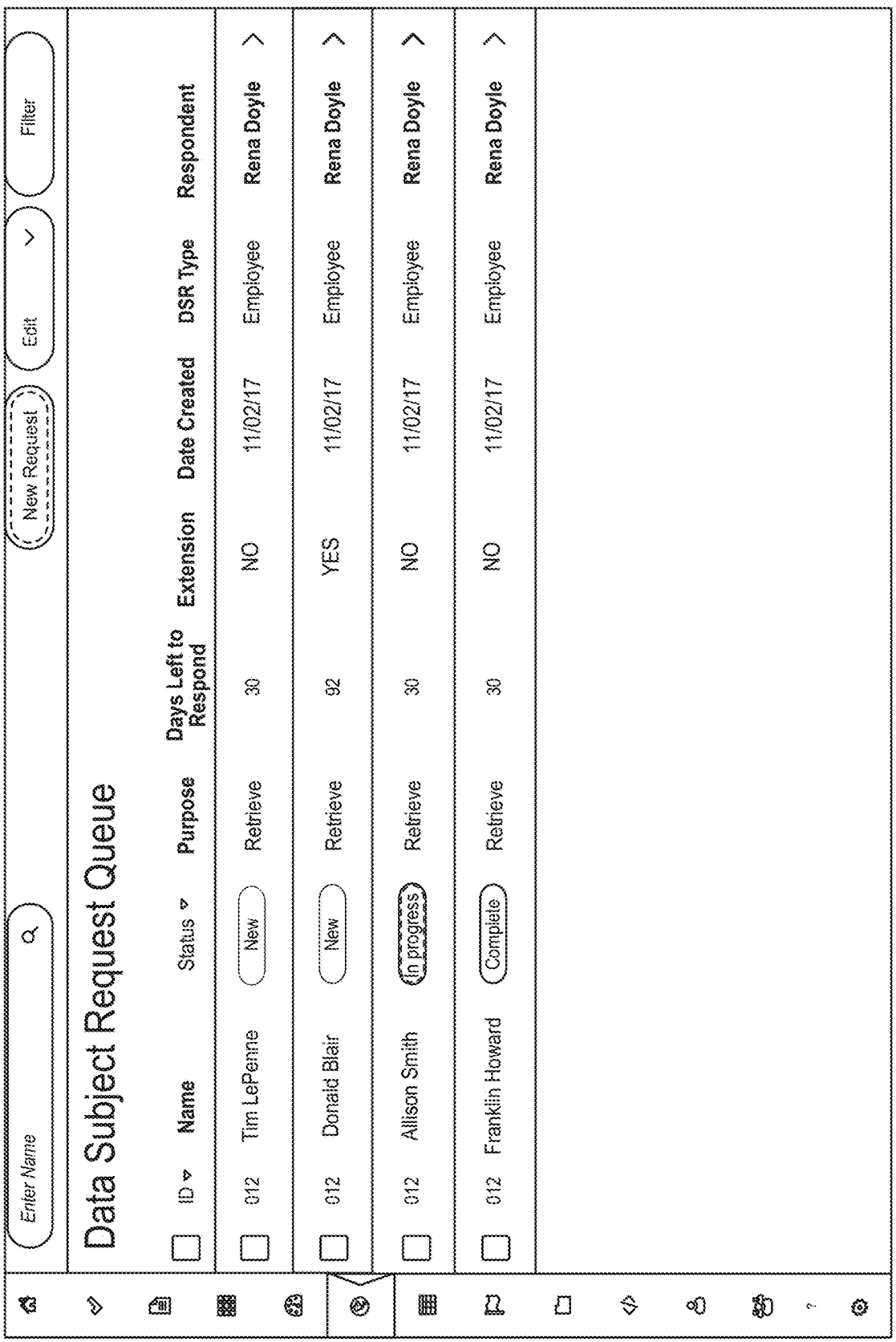

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Tim LePenne New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair New Retrieve 92 YES 11/02/17 Employee Rena Doyle
012 Allison Smith In progress Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Franklin Howard Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 27

From: OneTrust Privacy Officer
Sent: Sunday, February 19, 2017 9:27 PM EST
To: Allison Smith <asmith123456789@gmail.com>
Bcc: Amelia Davis <adavis09876@ACME.com>
Subject: *Your ACME Privacy Request is being Completed*

ACME CORPORATION

Data Response

Dear Allison,

Due to the complexity of this request, the response has been delayed

If you have any questions regarding your submission, please contact *Amelia Davis* via email or phone:
adavis09876@ACME.com
+00 123 123 9980

ACME Privacy
123 Main St.
Capital City, ST, USA 20219

+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 28

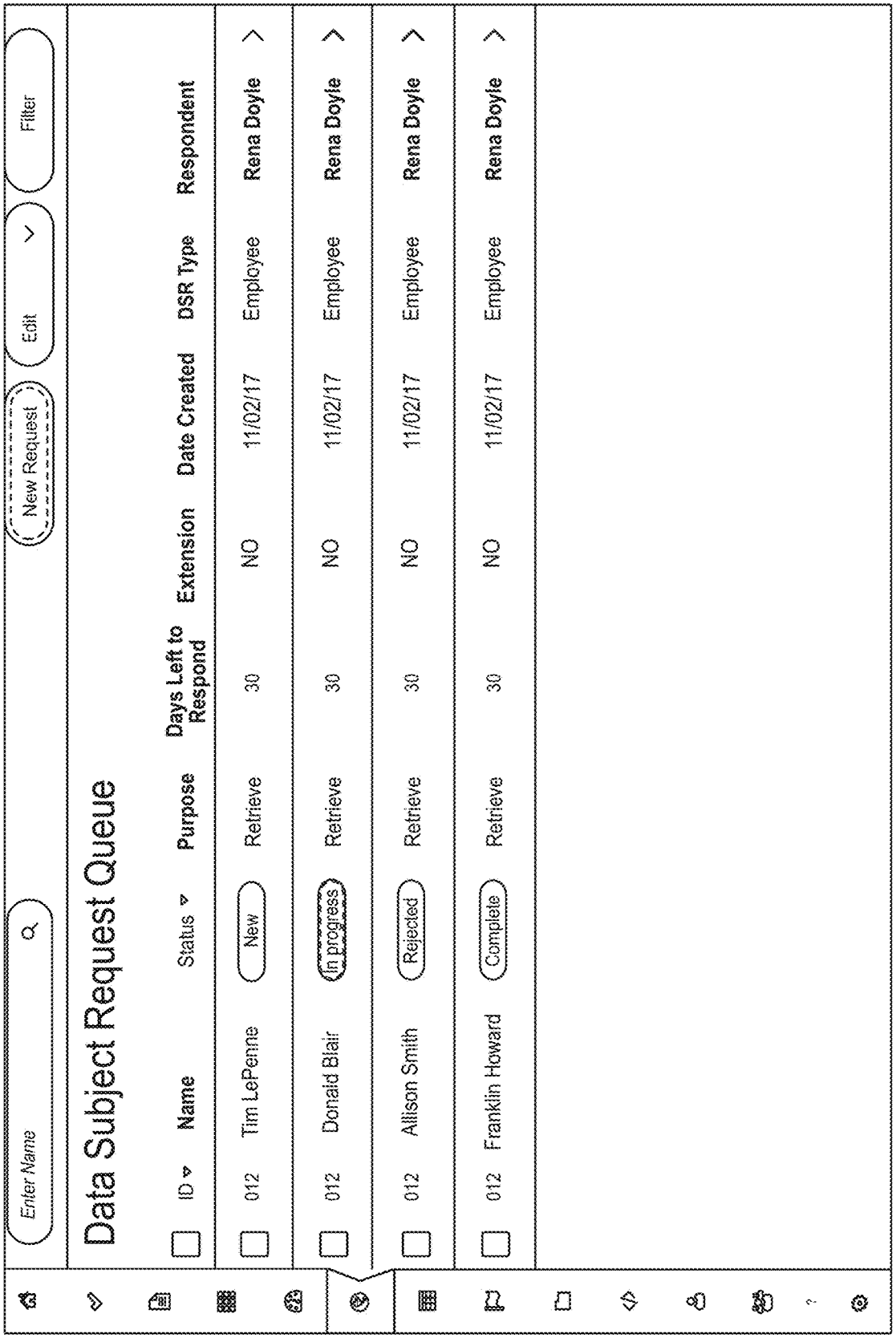

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012
Tim LePenne
New
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Donald Blair
In progress
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Allison Smith
Rejected
Retrieve
30
NO
11/02/17
Employee
Rena Doyle
012
Franklin Howard
Complete
Retrieve
30
NO
11/02/17
Employee
Rena Doyle

FIG. 29

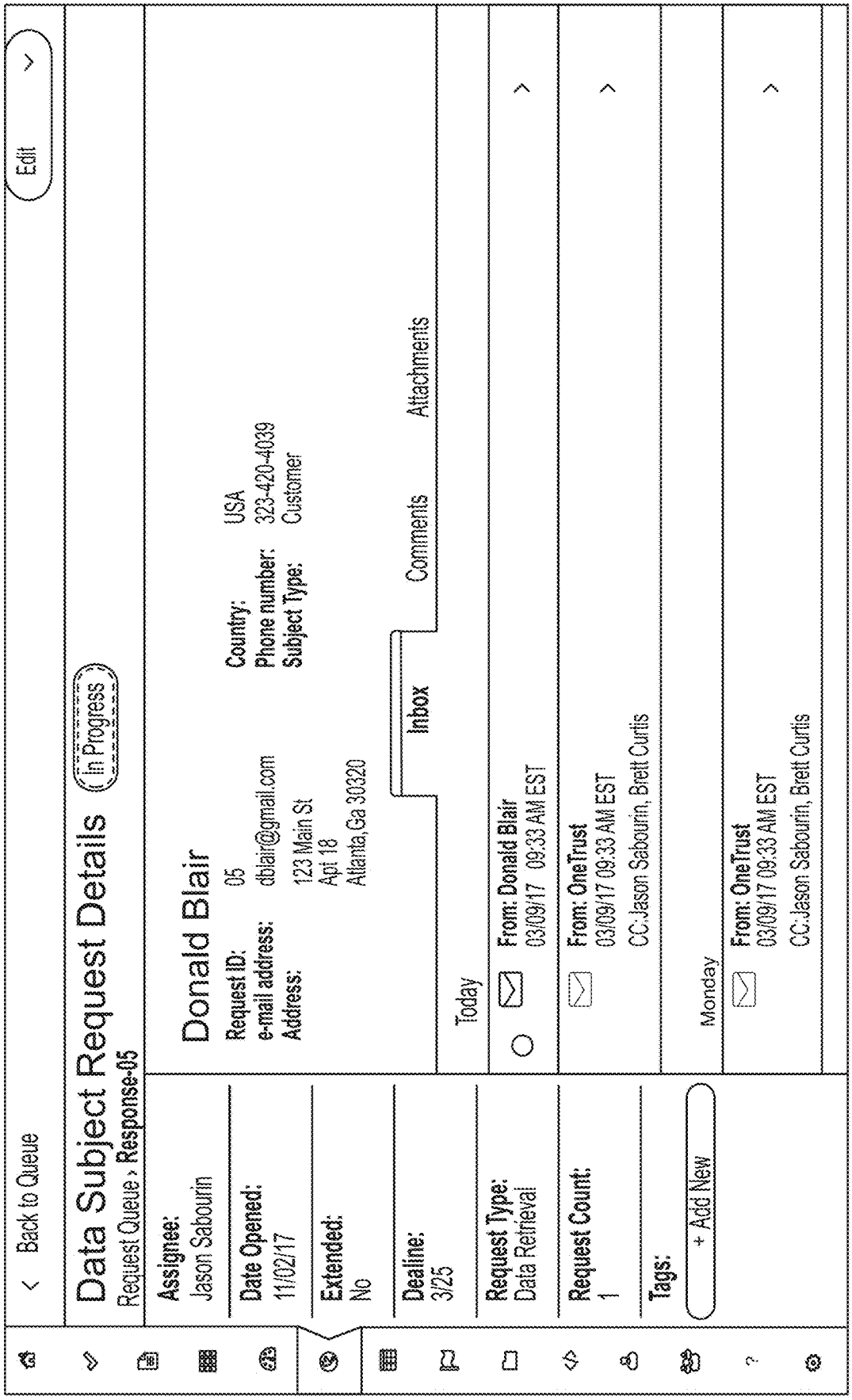

Back to Queue
Edit
Data Subject Request Details
In Progress
Request Queue › Response-05
Assignee:
Jason Sabourin
Date Opened:
11/02/17
Extended:
No
Deadline:
3/25
Request Type:
Data Retrieval
Request Count:
1
Tags:
+ Add New
Donald Blair
Request ID:
05
e-mail address:
dblair@gmail.com
Address:
123 Main St
Apt 18
Atlanta,Ga 30320
Country:
USA
Phone number:
323-420-4039
Subject Type:
Customer
Inbox
Comments
Attachments
Today
From: Donald Blair
03/09/17 09:33 AM EST
From: OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis
Monday
From: OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis

FIG. 30

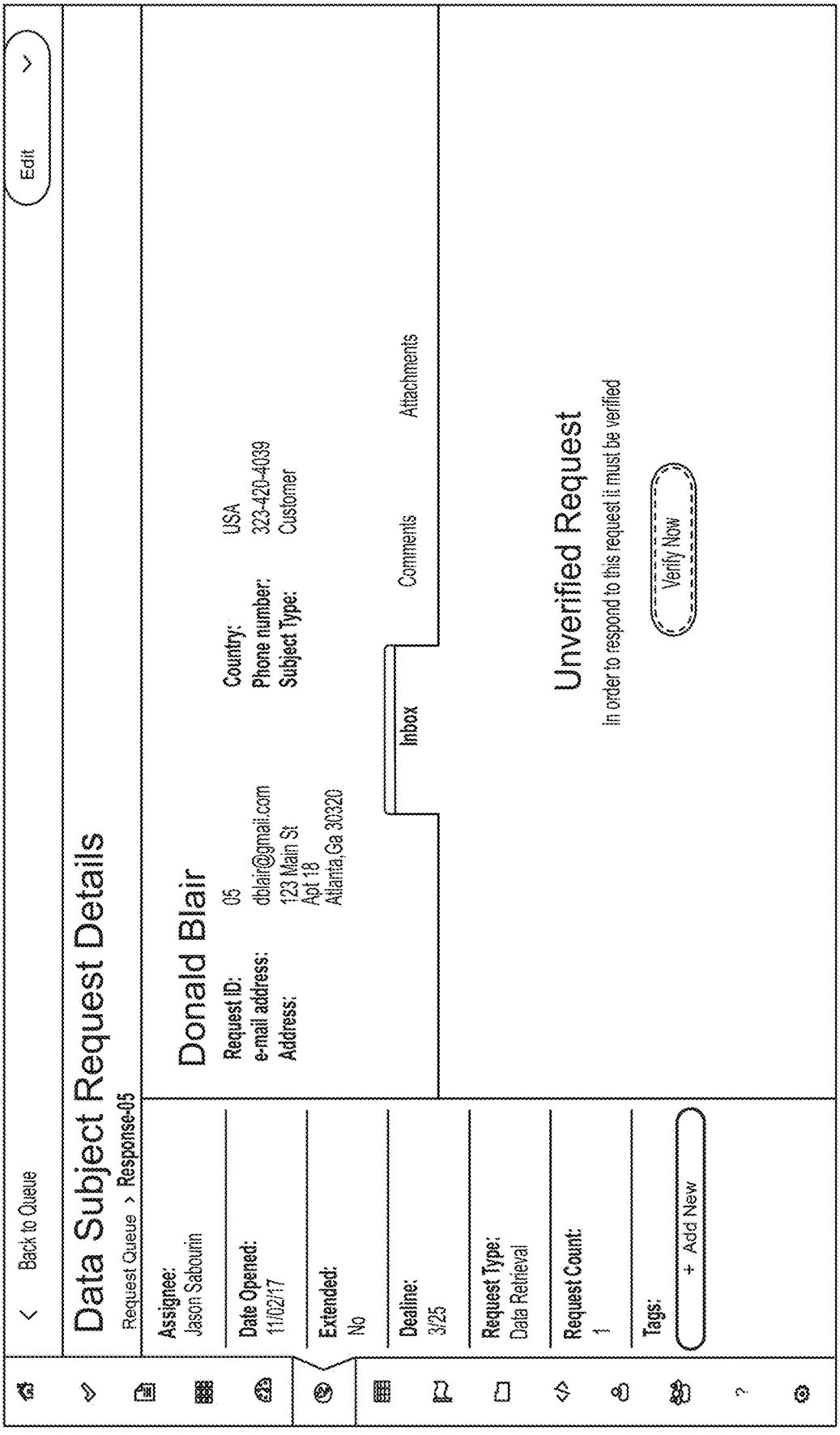

Back to Queue
Edit
Data Subject Request Details
Request Queue > Response-05
Assignee:
Jason Sabourin
Date Opened:
11/02/17
Extended:
No
Deadline:
3/25
Request Type:
Data Retrieval
Request Count:
1
Tags:
+ Add New
Donald Blair
Request ID: 05
e-mail address: dblair@gmail.com
Address: 123 Main St
Apt 18
Atlanta,Ga 30320
Country: USA
Phone number: 323-420-4039
Subject Type: Customer
Inbox
Comments
Attachments
Unverified Request
In order to respond to this request it must be verified
Verify Now

FIG. 31

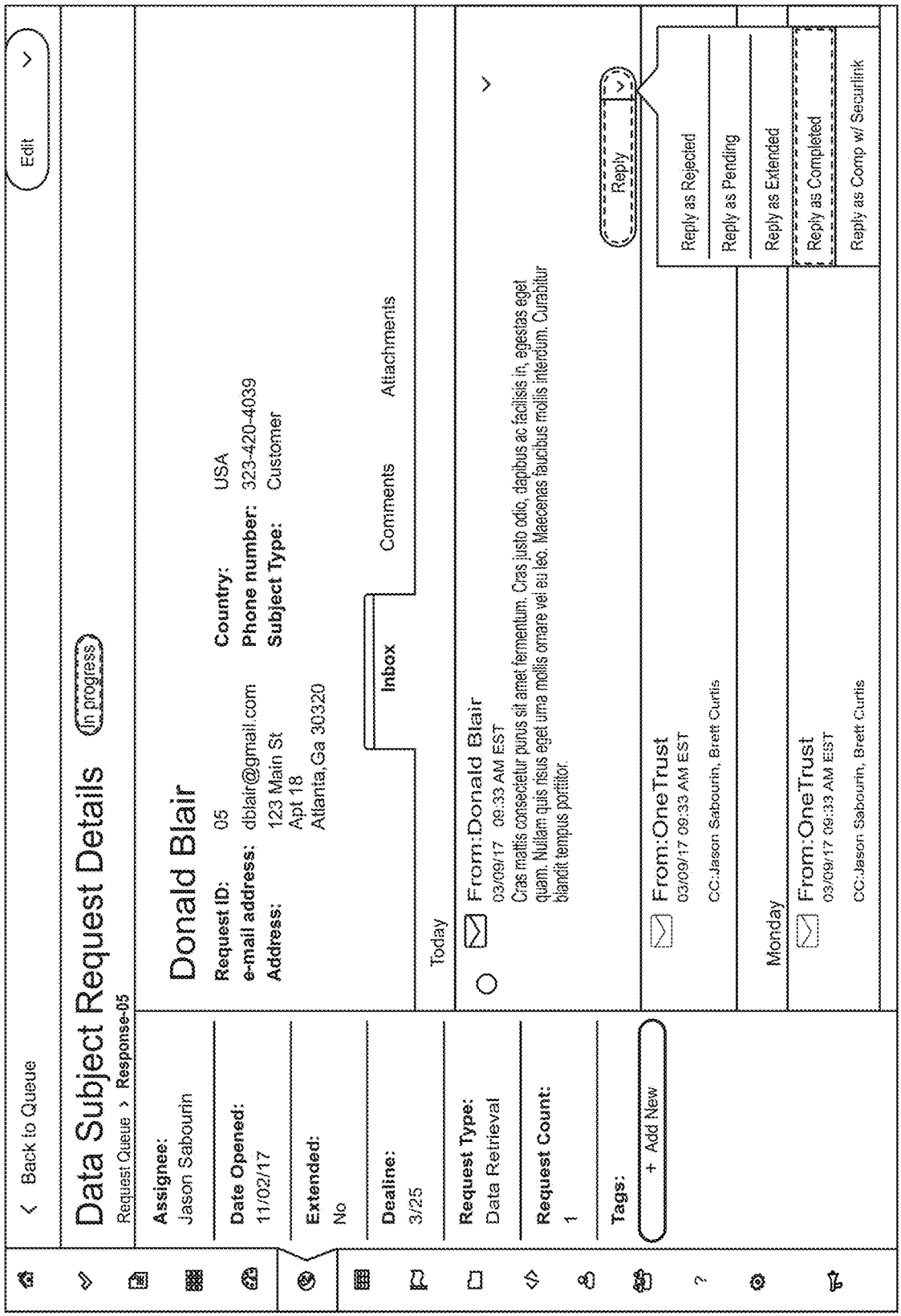

Back to Queue
Edit
Data Subject Request Details
In progress
Request Queue > Response-05
Assignee:
Jason Sabourin
Donald Blair
Request ID: 05
Country: USA
e-mail address: dblair@gmail.com
Phone number: 323-420-4039
Address: 123 Main St
Apt 18
Atlanta,Ga 30320
Subject Type: Customer
Date Opened:
11/02/17
Extended:
No
Deadline:
3/25
Request Type:
Data Retrieval
Request Count:
1
Tags:
+ Add New
Inbox
Comments
Attachments
Today
From:Donald Blair
03/09/17 09:33 AM EST
Cras mattis consectetur purus sit amet fermentum. Cras justo odio, dapibus ac facilisis in, egestas eget quam. Nullam quis risus eget urna mollis ornare vel eu leo. Maecenas faucibus mollis interdum. Curabitur blandit tempus porttitor.
Reply
From:OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis
Reply as Rejected
Reply as Pending
Reply as Extended
Reply as Completed
Reply as Comp w/ Securlink
Monday
From:OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis

FIG. 32

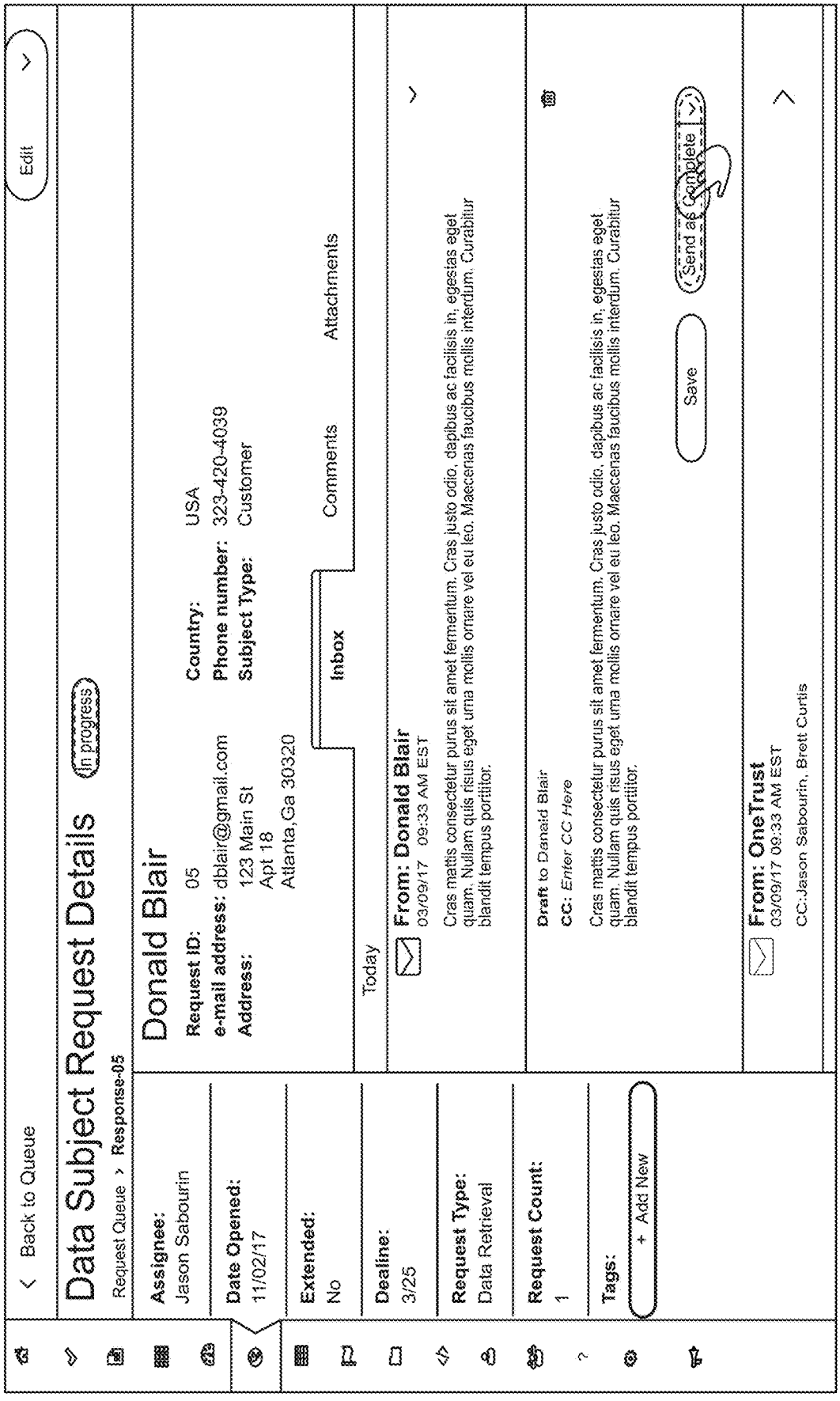

Back to Queue
Edit
Data Subject Request Details
In progress
Request Queue › Response-05
Donald Blair
Assignee:
Jason Sabourin
Request ID: 05
Country: USA
e-mail address: dblair@gmail.com
Phone number: 323-420-4039
Address: 123 Main St
Apt 18
Atlanta,Ga 30320
Subject Type: Customer
Date Opened:
11/02/17
Extended:
No
Deadline:
3/25
Request Type:
Data Retrieval
Request Count:
1
Tags:
+ Add New
Inbox
Comments
Attachments
Today
From: Donald Blair
03/09/17 09:33 AM EST
Cras mattis consectetur purus sit amet fermentum. Cras justo odio, dapibus ac facilisis in, egestas eget quam. Nullam quis risus eget urna mollis ornare vel eu leo. Maecenas faucibus mollis interdum. Curabitur blandit tempus portiitor.
Draft to Donald Blair
CC: Enter CC Here
Cras mattis consectetur purus sit amet fermentum. Cras justo odio, dapibus ac facilisis in, egestas eget quam. Nullam quis risus eget urna mollis ornare vel eu leo. Maecenas faucibus mollis interdum. Curabitur blandit tempus portiitor.
Save
Send as Complete
From: OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis

FIG. 33

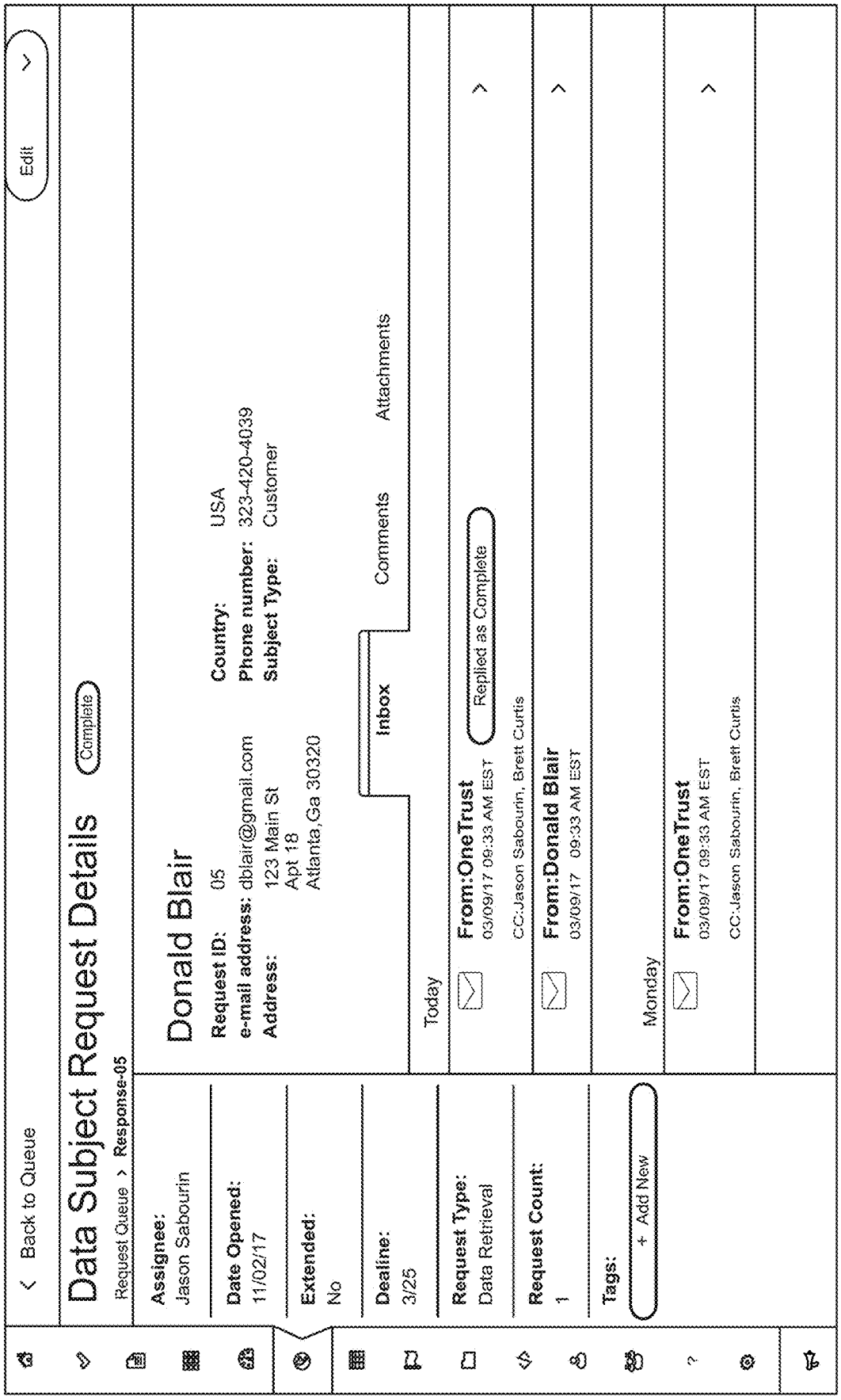

Back to Queue
Edit
Data Subject Request Details
Complete
Request Queue > Response-05
Assignee:
Jason Sabourin
Donald Blair
Request ID: 05
e-mail address: dblair@gmail.com
Address: 123 Main St
Apt 18
Atlanta,Ga 30320
Country: USA
Phone number: 323-420-4039
Subject Type: Customer
Date Opened:
11/02/17
Extended:
No
Deadline:
3/25
Request Type:
Data Retrieval
Request Count:
1
Tags:
+ Add New
Inbox
Comments
Attachments
Today
From:OneTrust
03/09/17 09:33 AM EST
Replied as Complete
CC:Jason Sabourin, Brett Curtis
From:Donald Blair
03/09/17 09:33 AM EST
Monday
From:OneTrust
03/09/17 09:33 AM EST
CC:Jason Sabourin, Brett Curtis

FIG. 34

From: OneTrust Privacy Officer
Sent: Sunday, February 19, 2017 9:27 PM EST
To: Joe Lopez <jlopez123456789@gmail.com>
Bcc: Amelia Davis <adavis09876@ACME.com>
Subject: *Your ACME Privacy Request is Completed*

ACME CORPORATION

Data Response

Dear Joe,

Your privacy-related request has been completed. In order to access the data you requested, please click the secure link below.

http://www.securelink.onetrust.com/1124ahawlu091284

If you have any questions regarding your submission, please contact *Amelia Davis* via email or phone:
adavis09876@ACME.com
+00 123 123 9980

Here are the details of your request:

Request ID: 5
Date Submitted: 2/21/2017 10:35AM EST
I am a(n): Customer
My request involves: Opting Out
First Name*: Joe
Last Name*: Lopez
Email Address*: Jlopez123456789@gmail.com
Telephone: XXXXXXXXX
Addr Line 1: XXXXXXXXXX
Addr Line 2: XXXXXXXXXX
City: XXXXXXXXXX
Count of Residence*: XXXXXXXXXX
Details of my request:
Send me my Data

If you have any questions regarding your submission, please contact *Amelia Davis* via email or phone:
adavis09876@ACME.com
+00 123 123 9980

ACME Privacy
123 Main St.
Capital City, ST, USA 20219

+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 35

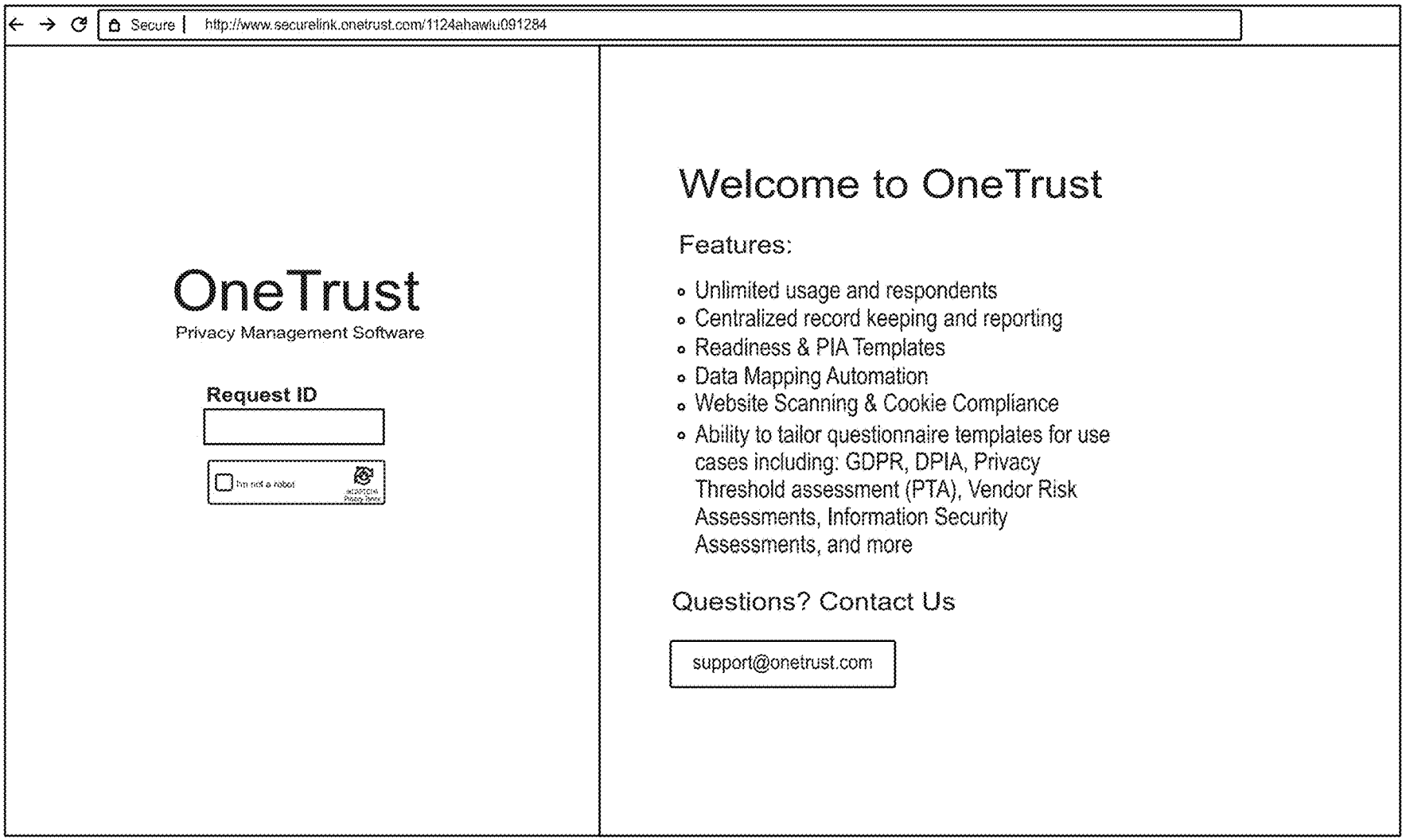

Secure
http://www.securelink.onetrust.com/1124ahawlu091284
OneTrust
Privacy Management Software
Request ID
I'm not a robot
Welcome to OneTrust
Features:
Unlimited usage and respondents
Centralized record keeping and reporting
Readiness & PIA Templates
Data Mapping Automation
Website Scanning & Cookie Compliance
Ability to tailor questionnaire templates for use cases including: GDPR, DPIA, Privacy Threshold assessment (PTA), Vendor Risk Assessments, Information Security Assessments, and more
Questions? Contact Us
support@onetrust.com

FIG. 36

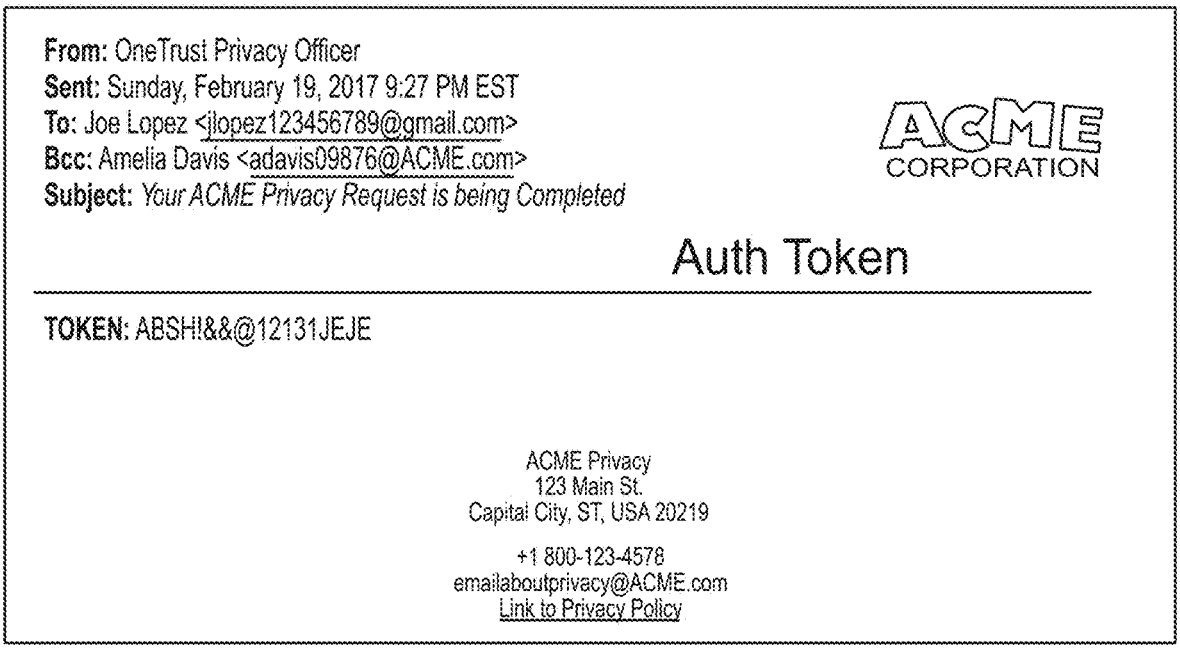

From: OneTrust Privacy Officer
Sent: Sunday, February 19, 2017 9:27 PM EST
To: Joe Lopez <jlopez123456789@gmail.com>
Bcc: Amelia Davis <adavis09876@ACME.com>
Subject: Your ACME Privacy Request is being Completed
ACME CORPORATION
Auth Token
TOKEN: ABSH!&&@12131JEJE
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 37

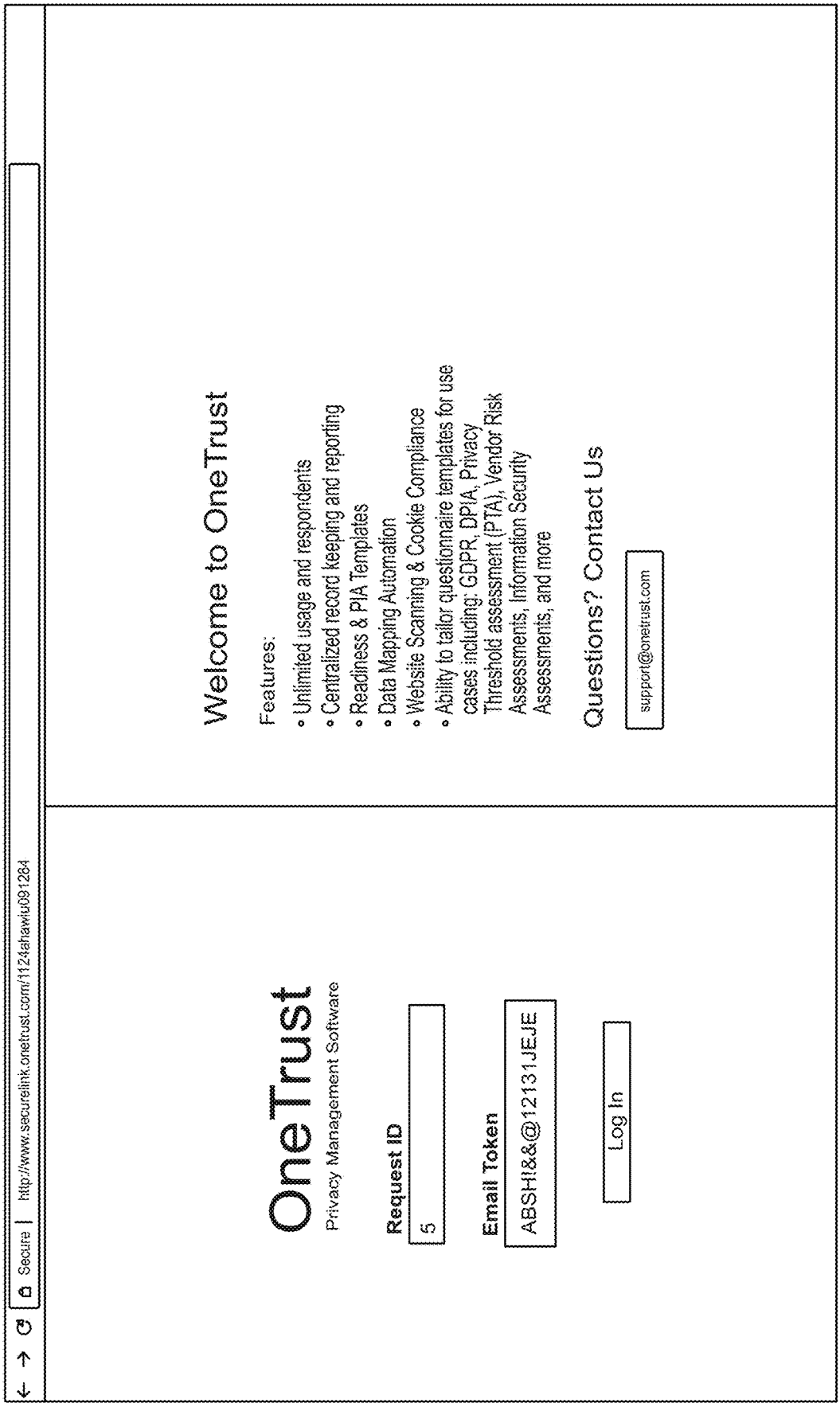

Secure | http://www.securelink.onetrust.com/1124ahawiu091284
OneTrust
Privacy Management Software
Request ID
5
Email Token
ABSHI&&@12131JEJE
Log In
Welcome to OneTrust
Features:
• Unlimited usage and respondents
• Centralized record keeping and reporting
• Readiness & PIA Templates
• Data Mapping Automation
• Website Scanning & Cookie Compliance
• Ability to tailor questionnaire templates for use cases including: GDPR, DPIA, Privacy Threshold assessment (PTA), Vendor Risk Assessments, Information Security Assessments, and more
Questions? Contact Us
support@onetrust.com

FIG. 38

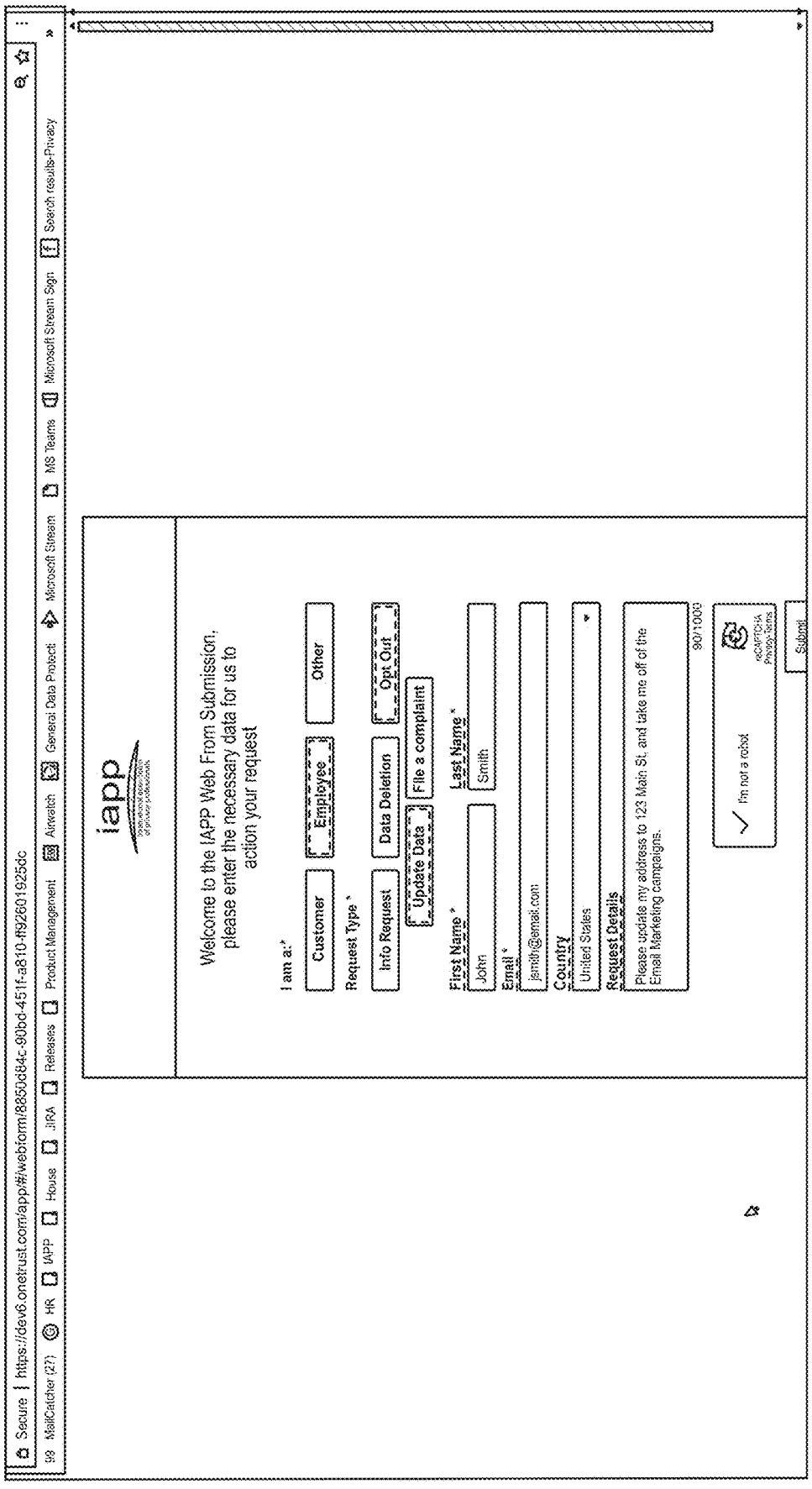

Secure | https://dev6.onetrust.com/app/#/webform/8850d84c-90bd-451f-a810-ff92601925dc
MailCatcher (27)
HR
IAPP
House
JIRA
Releases
Product Management
Airwatch
General Data Protect
Microsoft Stream
MS Teams
Microsoft Stream Sign
Search results-Privacy
iapp
Welcome to the IAPP Web From Submission, please enter the necessary data for us to action your request
I am a:*
Customer
Employee
Other
Request Type *
Info Request
Data Deletion
Opt Out
Update Data
File a complaint
First Name *
John
Last Name *
Smith
Email *
jsmith@email.com
Country
United States
Request Details
Please update my address to 123 Main St. and take me off of the Email Marketing campaigns.
90/1000
I'm not a robot
reCAPTCHA
Privacy-Terms
Submit

FIG. 39

From: Generitech Privacy officer
Sent: Monday, February 20,2017 9:27 PM EST
To: Alison Smith <asmith 123456789@gmail.com>
Bcc: Amelia Davis <adavis09876@generitech.com>
Subject: Your Generitech Privacy Request is completed

OneTrust
Privacy Management Software

Data Subject Request Assignment

Dear Joe,

The following data subject request has been filed, and you have been identified as someone who knows how to fulfill the request. Please click the link below, in order to fulfill the request

Click here to access the request

Access Request

If you have questions regarding your submission, please contact Amelia Davis via email or phone:

adavis09876@ACME.com
+00 123 123 9980

Generitech Privacy
123 Main St.
Capital City, ST, USA 20219

+1 800-123-4578
emailaboutprivacy@generitech.com
Link to Privacy Policy

FIG. 40

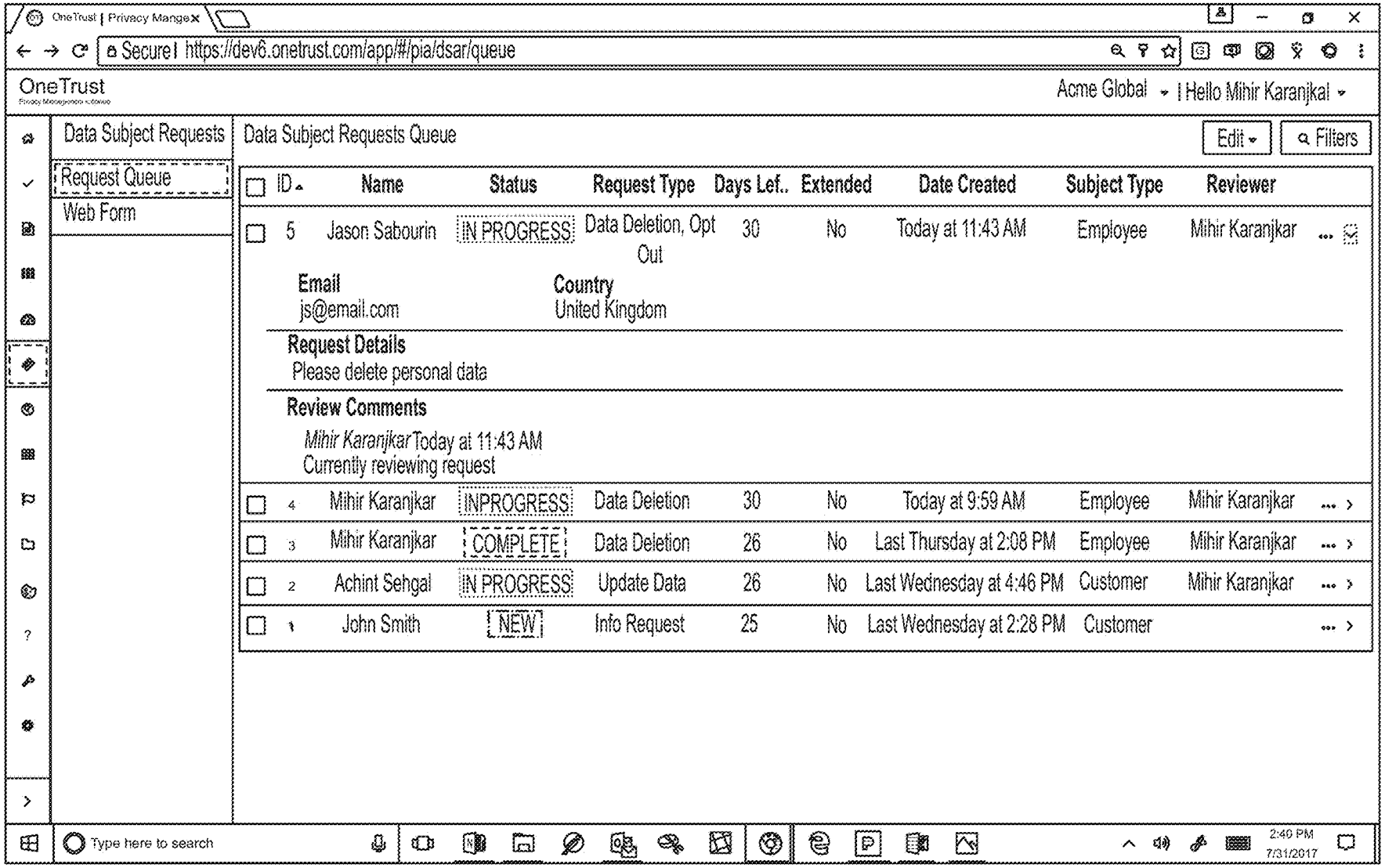

OneTrust | Privacy Mange
Secure | https://dev6.onetrust.com/app/#/pia/dsar/queue
OneTrust
Acme Global | Hello Mihir Karanjkal
Data Subject Requests
Request Queue
Web Form
Data Subject Requests Queue
Edit
Filters
ID
Name
Status
Request Type
Days Lef..
Extended
Date Created
Subject Type
Reviewer
5 Jason Sabourin IN PROGRESS Data Deletion, Opt Out 30 No Today at 11:43 AM Employee Mihir Karanjkar
Email
js@email.com
Country
United Kingdom
Request Details
Please delete personal data
Review Comments
Mihir Karanjkar Today at 11:43 AM
Currently reviewing request
4 Mihir Karanjkar INPROGRESS Data Deletion 30 No Today at 9:59 AM Employee Mihir Karanjkar
3 Mihir Karanjkar COMPLETE Data Deletion 26 No Last Thursday at 2:08 PM Employee Mihir Karanjkar
2 Achint Sehgal IN PROGRESS Update Data 26 No Last Wednesday at 4:46 PM Customer Mihir Karanjkar
1 John Smith NEW Info Request 25 No Last Wednesday at 2:28 PM Customer
Type here to search
2:40 PM
7/31/2017

FIG. 41

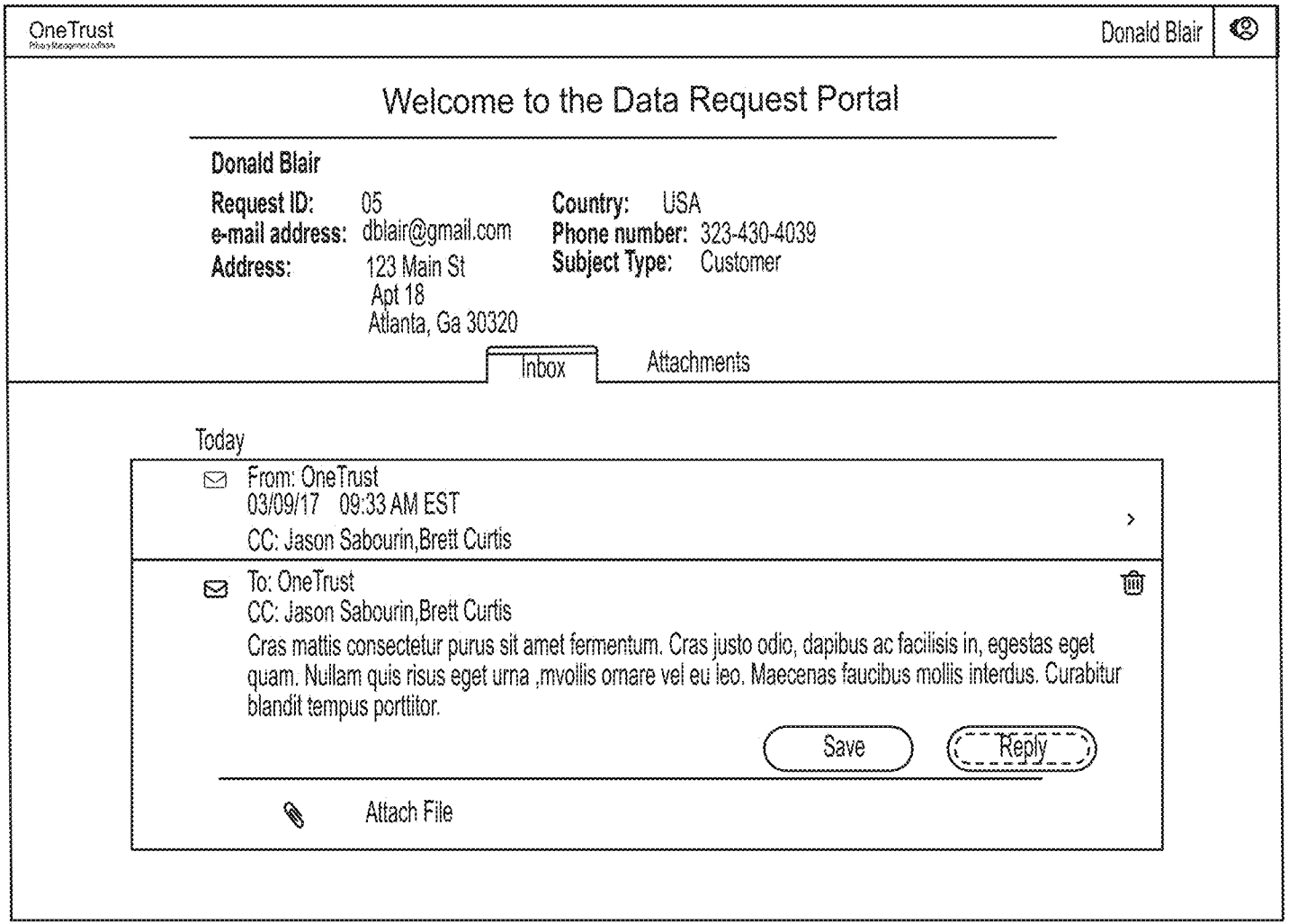

OneTrust
Donald Blair
Welcome to the Data Request Portal
Donald Blair
Request ID: 05
e-mail address: dblair@gmail.com
Address: 123 Main St
Apt 18
Atlanta, Ga 30320
Country: USA
Phone number: 323-430-4039
Subject Type: Customer
Inbox
Attachments
Today
From: OneTrust
03/09/17 09:33 AM EST
CC: Jason Sabourin,Brett Curtis
To: OneTrust
CC: Jason Sabourin,Brett Curtis
Cras mattis consectetur purus sit amet fermentum. Cras justo odio, dapibus ac facilisis in, egestas eget quam. Nullam quis risus eget urna ,mvollis ornare vel eu leo. Maecenas faucibus mollis interdus. Curabitur blandit tempus porttitor.
Save
Reply
Attach File

FIG. 42

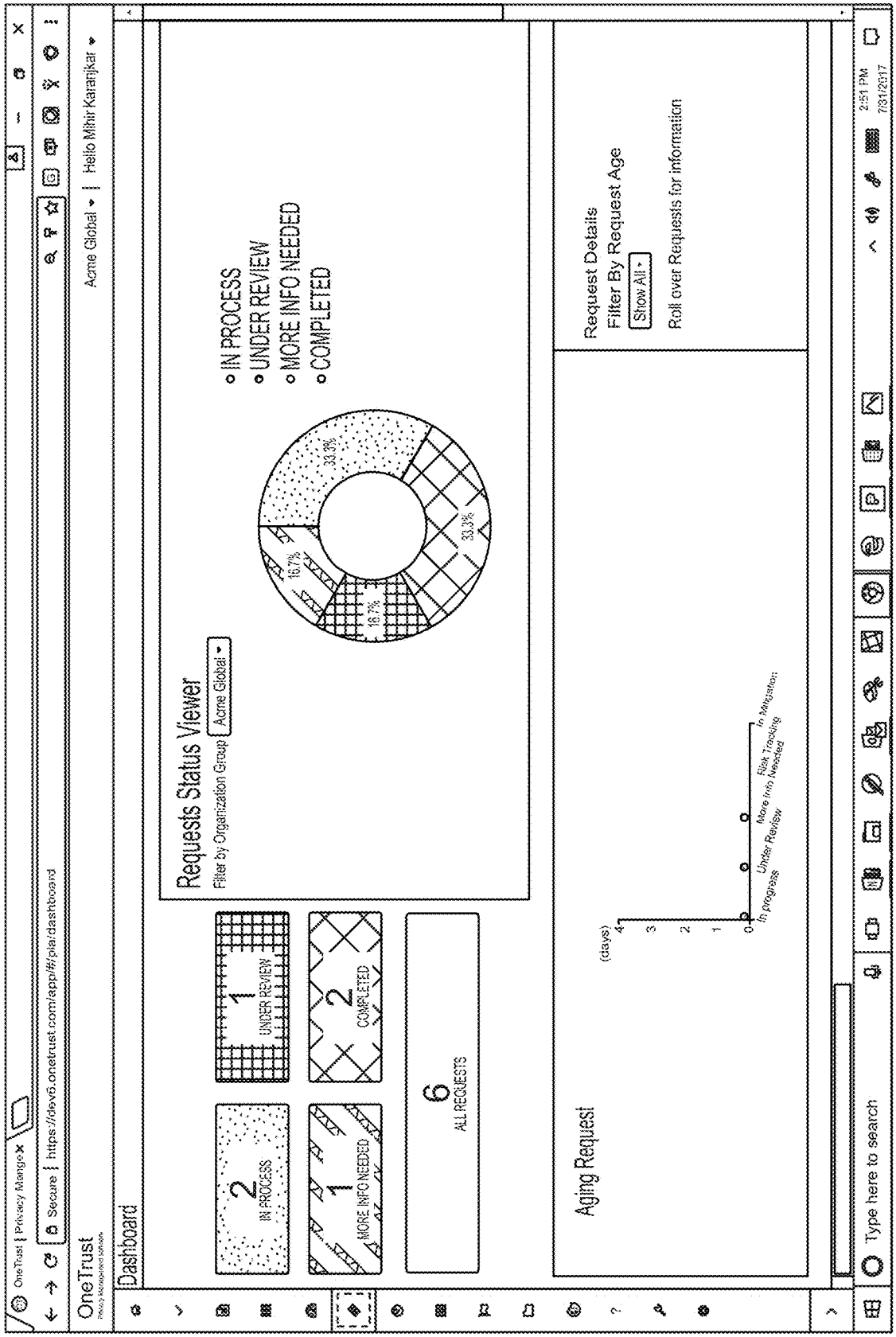
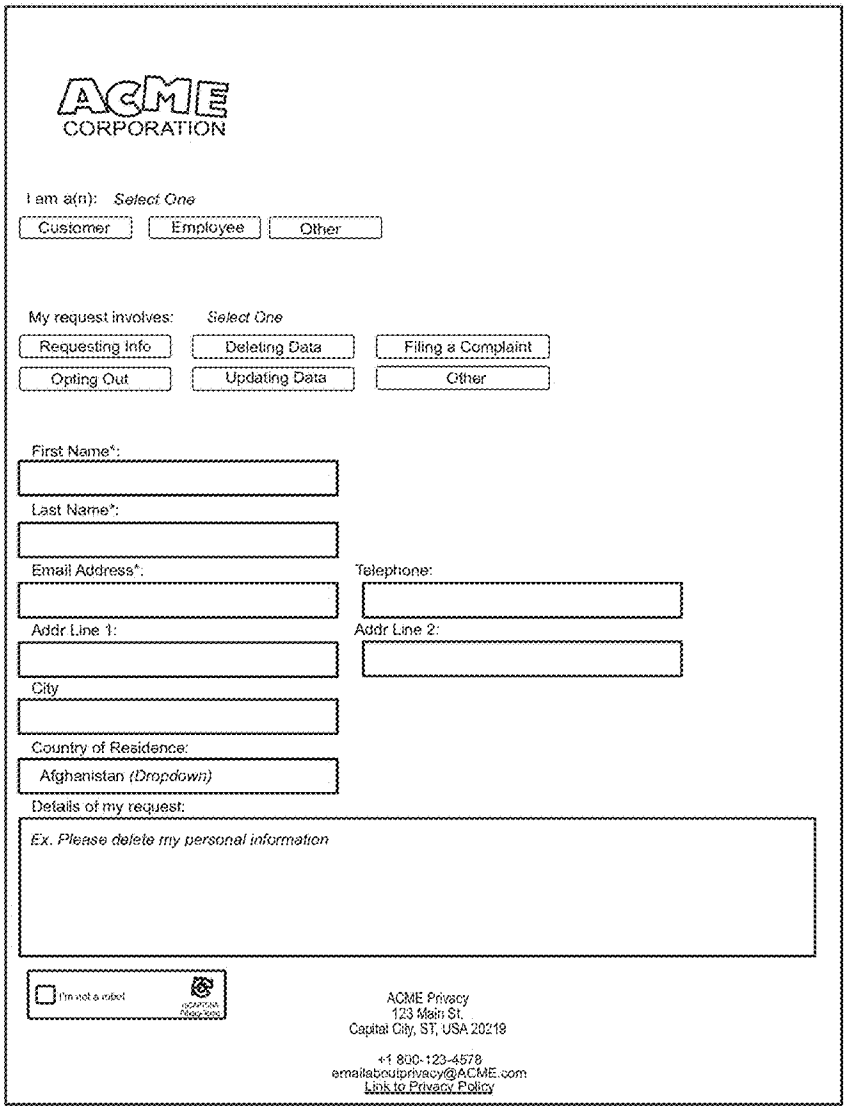

OneTrust | Privacy Mange
Secure | https://dev6.onetrust.com/app/#/pia/dashboard
OneTrust
Acme Global | Hello Mihir Karanjkar
Dashboard
2 IN PROCESS
1 UNDER REVIEW
1 MORE INFO NEEDED
2 COMPLETED
6 ALL REQUESTS
Requests Status Viewer
Filter by Organization Group Acme Global
IN PROCESS
UNDER REVIEW
MORE INFO NEEDED
COMPLETED
33.3%
16.7%
16.7%
33.3%
Aging Request
(days)
In progress
Under Review
More Info Needed
Risk Tracking
In Migration
Request Details
Filter By Request Age
Show All
Roll over Requests for information
Type here to search
2:51 PM
7/31/2017

FIG. 43

Secure | https://onetrust.com/privacy-policy/
ACME CORPORATION
Products
Services
Pricing
Company
Partners
Resources
Blog
Contact
RFP Template
Free Trial
Request Demo
Privacy Policy
Effective Date: 17 April 2017
Policy Pages
Privacy Policy
Cookie Policy
Submit a Privacy Related Request
We at OneTrust LLC and OneTrust Technology Limited (collectively, "OneTrust," "we" and "us") know you care about how your personal information is used and shared, and we take your privacy seriously. Please read the following to learn more about how we collect, store, use and disclose information about you when you interact or use any of the following websites: www.onetrust.com, www.cookielaw.org, www.optanon.com, www.governor.co.uk, and https://cookiepedia.co.uk/ (collectively the "Websites") or any related events, trade shows, sales or marketing, and/or if you use any of our products, services or applications (including any trial) (collectively the "Services") in any manner.
What does this Privacy Policy cover?
This Privacy Policy covers our treatment of information that we gather when you are accessing or

FIG. 44


ACME
CORPORATION
I am a(n): Select One
Customer
Employee
Other
My request involves: Select One
Requesting Info
Deleting Data
Filing a Complaint
Opting Out
Updating Data
Other
First Name*:
Last Name*:
Email Address*:
Telephone:
Addr Line 1:
Addr Line 2:
City
Country of Residence:
Afghanistan (Dropdown)
Details of my request:
Ex. Please delete my personal information
I'm not a robot
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

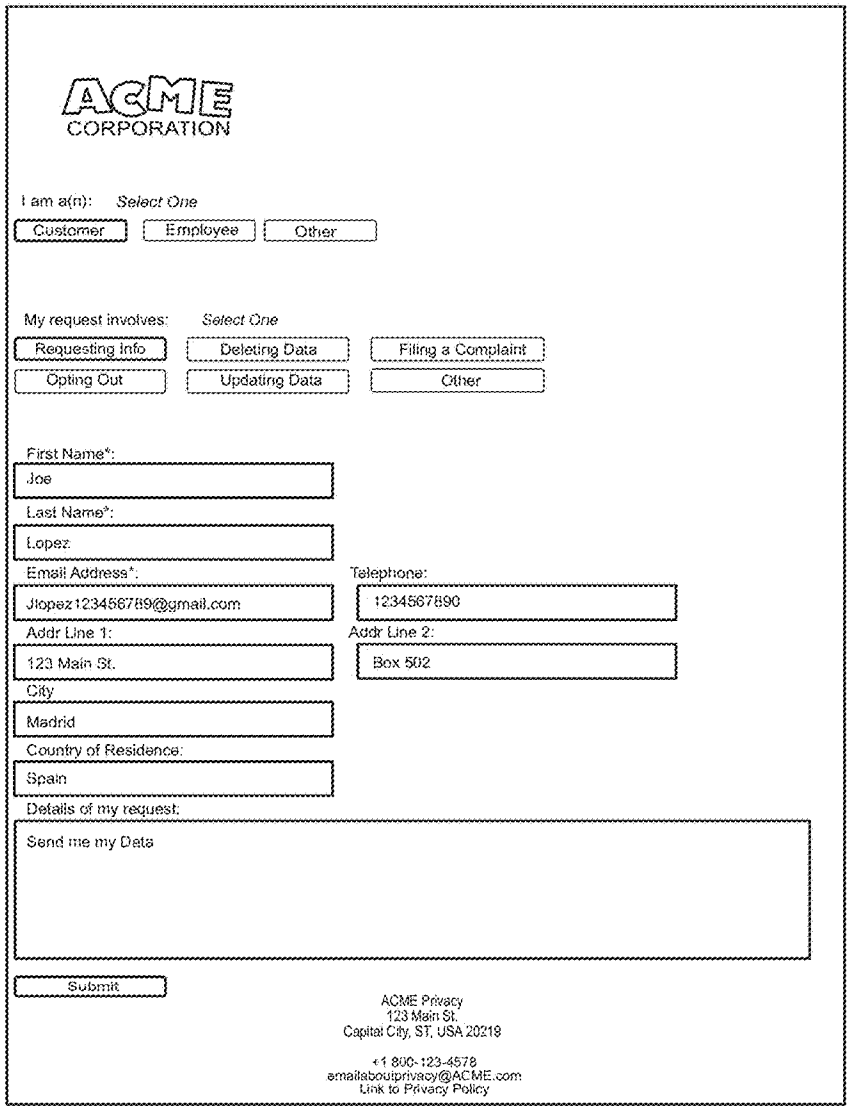
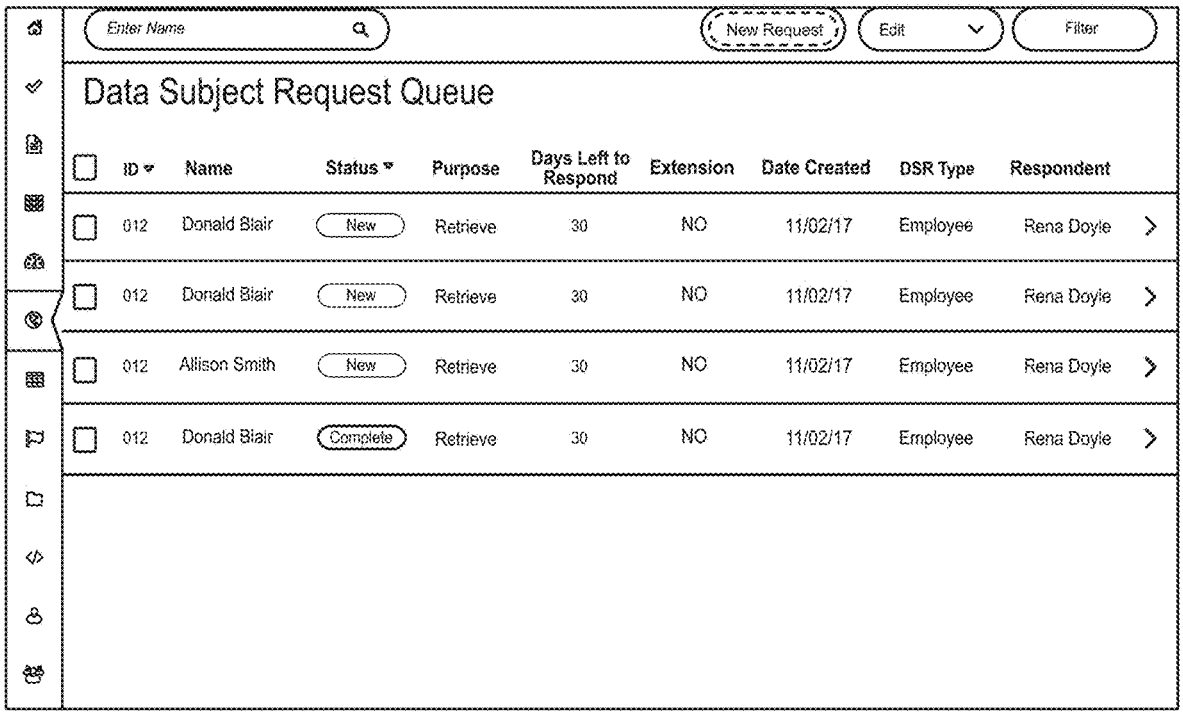

ACME
CORPORATION
I am a(n): Select One
Customer
Employee
Other
My request involves: Select One
Requesting Info
Deleting Data
Filing a Complaint
Opting Out
Updating Data
Other
First Name*:
Joe
Last Name*:
Lopez
Email Address*:
Jlopez123456789@gmail.com
Telephone:
12345678900
Addr Line 1:
123 Main St.
Addr Line 2:
Box 502
City
Madrid
Country of Residence:
Spain
Details of my request:
Send me my Data
Submit
ACME Privacy
123 Main St.
Capital City, ST, USA 20219
+1 800-123-4578
emailaboutprivacy@ACME.com
Link to Privacy Policy

FIG. 45

Verify Your Identity
Name: Joe Lopez
To verify your identity, please answer the following questions.
• Which of the following STREETS have you NEVER lived or used as your address?
ALL OF THE ABOVE
• With which of the following PEOPLE are you most closely associated?
NONE OF THE ABOVE
• Which of the following CITIES have you PREVIOUSLY OR CURRENTLY used as your address?
NONE OF THE ABOVE

FIG. 46


Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Allison Smith New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

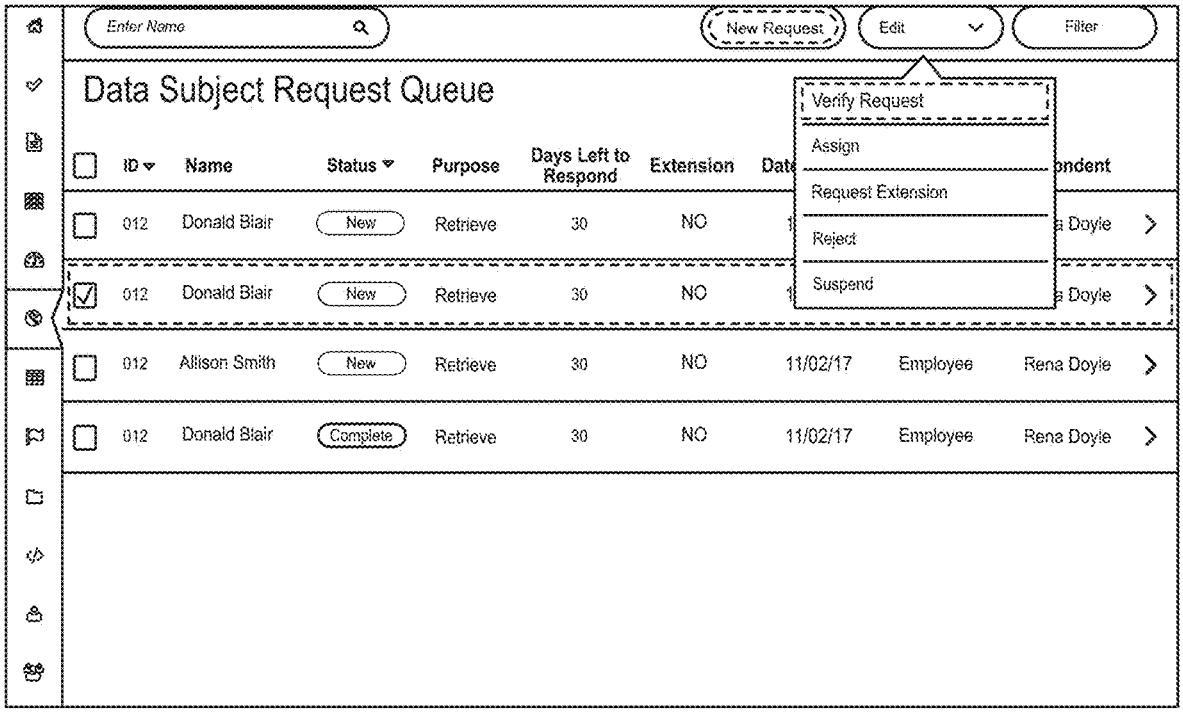
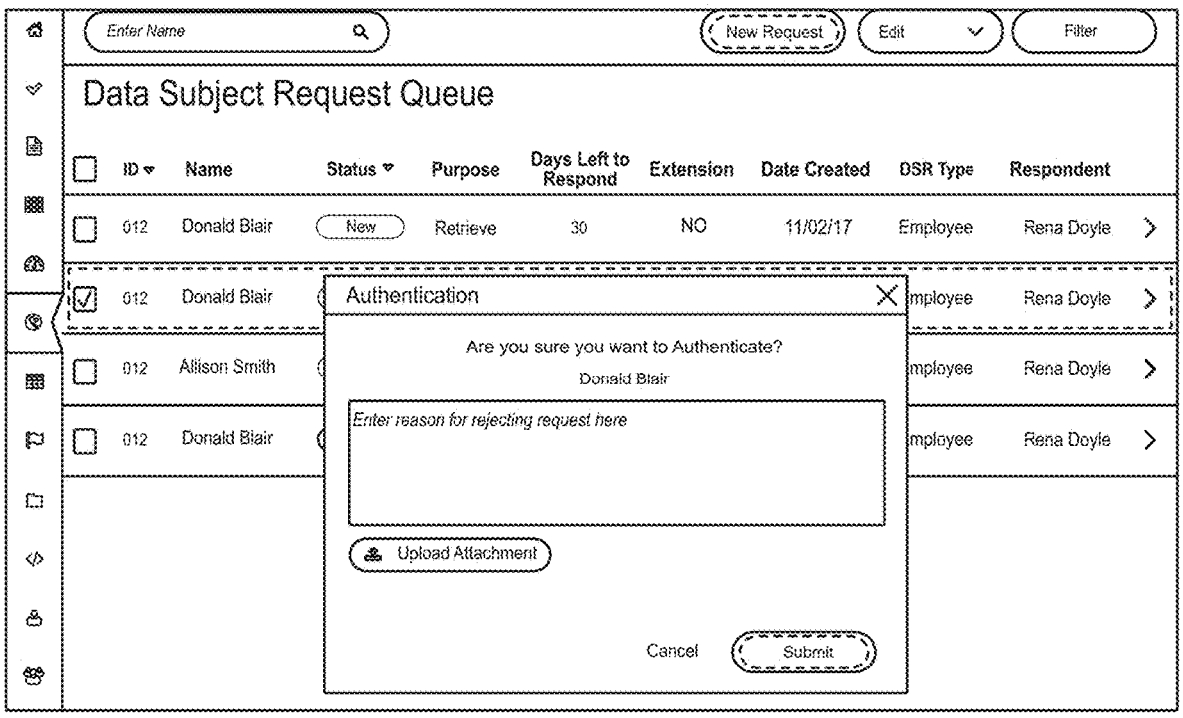

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
Verify Request
Assign
Request Extension
Reject
Suspend
ID
Name
Status
Purpose
Days Left to Respond
Extension
012 Donald Blair New Retrieve 30 NO
012 Donald Blair New Retrieve 30 NO
012 Allison Smith New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair Complete Retrieve 30 NO 11/02/17 Employee Rena Doyle

FIG. 47


Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair
012 Allison Smith
012 Donald Blair
Authentication
Are you sure you want to Authenticate?
Donald Blair
Enter reason for rejecting request here
Upload Attachment
Cancel
Submit

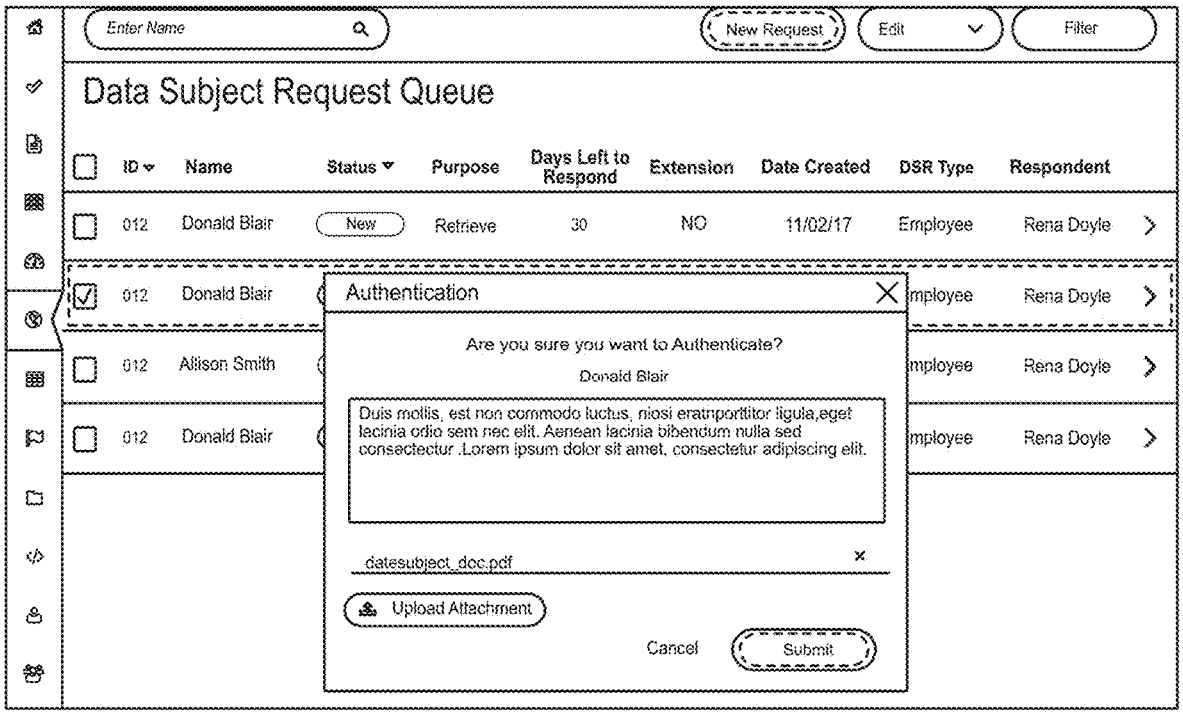

Enter Name
New Request
Edit
Filter
Data Subject Request Queue
ID
Name
Status
Purpose
Days Left to Respond
Extension
Date Created
DSR Type
Respondent
012 Donald Blair New Retrieve 30 NO 11/02/17 Employee Rena Doyle
012 Donald Blair
012 Allison Smith
012 Donald Blair
Authentication
Are you sure you want to Authenticate?
Donald Blair
Duis mollis, est non commodo luctus, nisi eratnporttitor ligula,eget lacinia odio sem nec elit. Aenean lacinia bibendum nulla sed consectectur .Lorem ipsum dolor sit amet, consectetur adipiscing elit.
datesubject_doc.pdf
Upload Attachment
Cancel
Submit

FIG. 48

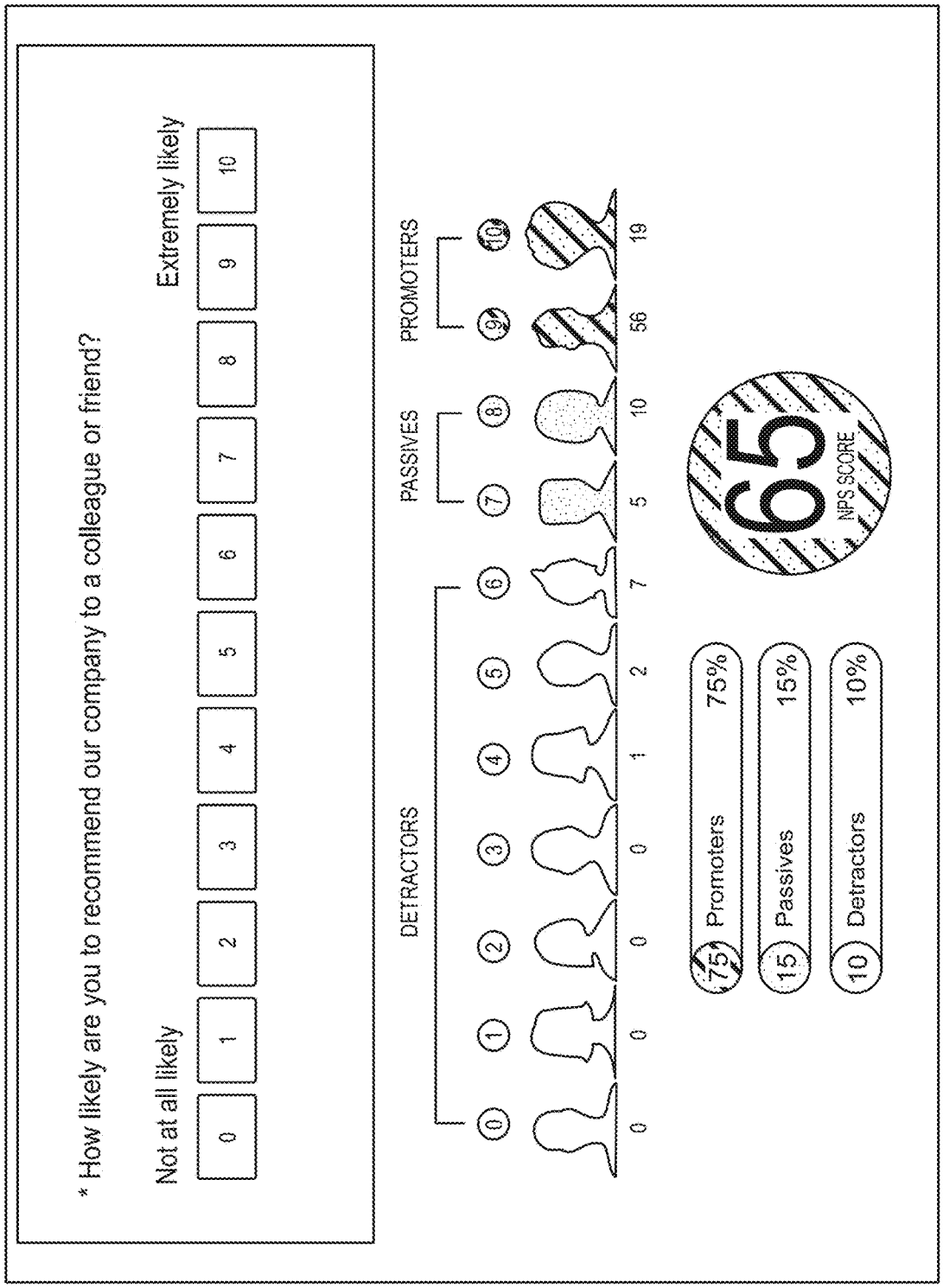

* How likely are you to recommend our company to a colleague or friend?
Not at all likely
Extremely likely
0
1
2
3
4
5
6
7
8
9
10
DETRACTORS
PASSIVES
PROMOTERS
0 0 0 0 1 2 7 5 10 56 19
75 Promoters 75%
15 Passives 15%
10 Detractors 10%
65
NPS SCORE

FIG. 49

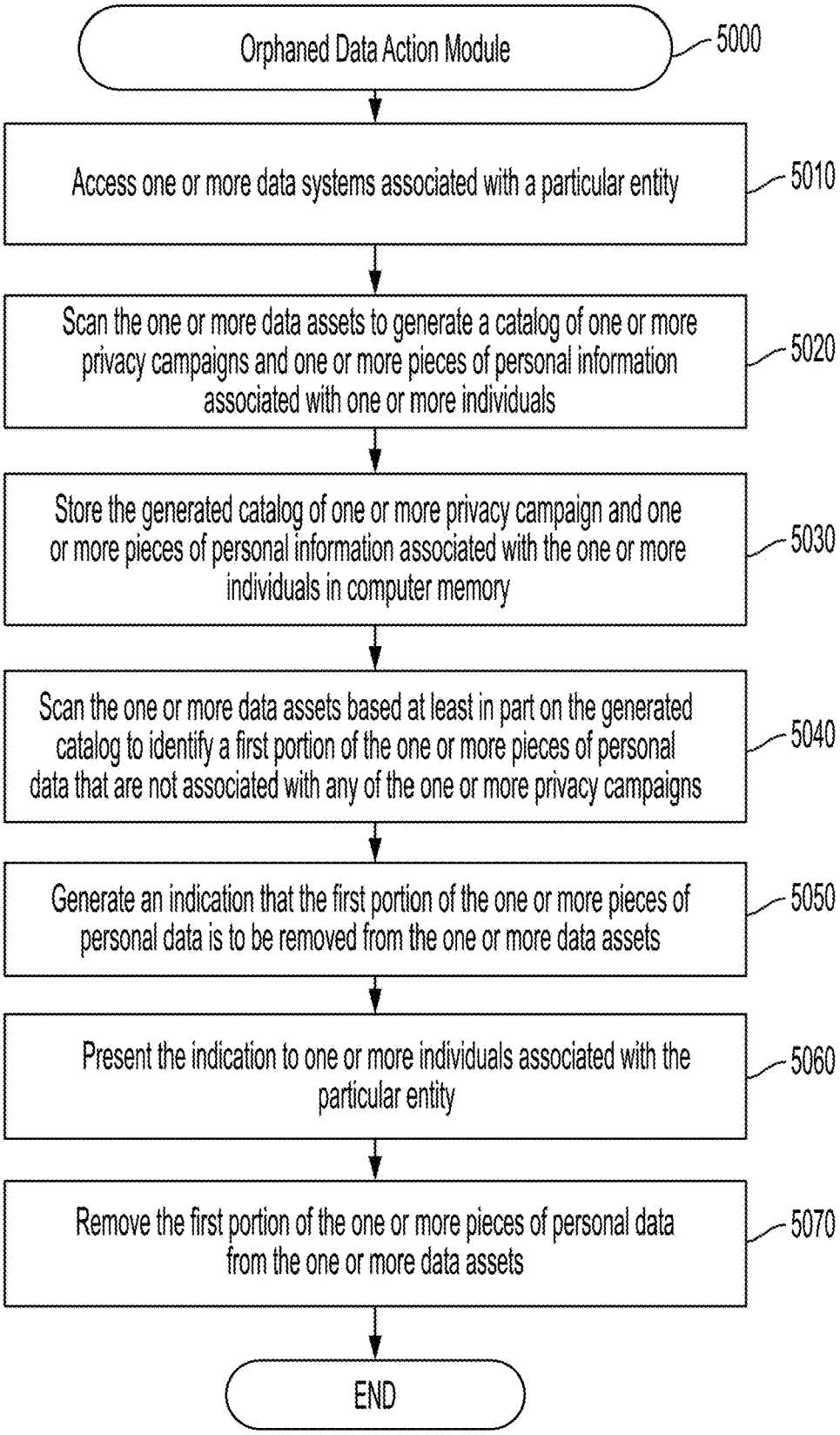

Orphaned Data Action Module
5000
Access one or more data systems associated with a particular entity
5010
Scan the one or more data assets to generate a catalog of one or more privacy campaigns and one or more pieces of personal information associated with one or more individuals
5020
Store the generated catalog of one or more privacy campaign and one or more pieces of personal information associated with the one or more individuals in computer memory
5030
Scan the one or more data assets based at least in part on the generated catalog to identify a first portion of the one or more pieces of personal data that are not associated with any of the one or more privacy campaigns
5040
Generate an indication that the first portion of the one or more pieces of personal data is to be removed from the one or more data assets
5050
Present the indication to one or more individuals associated with the particular entity
5060
Remove the first portion of the one or more pieces of personal data from the one or more data assets
5070
END

FIG. 50

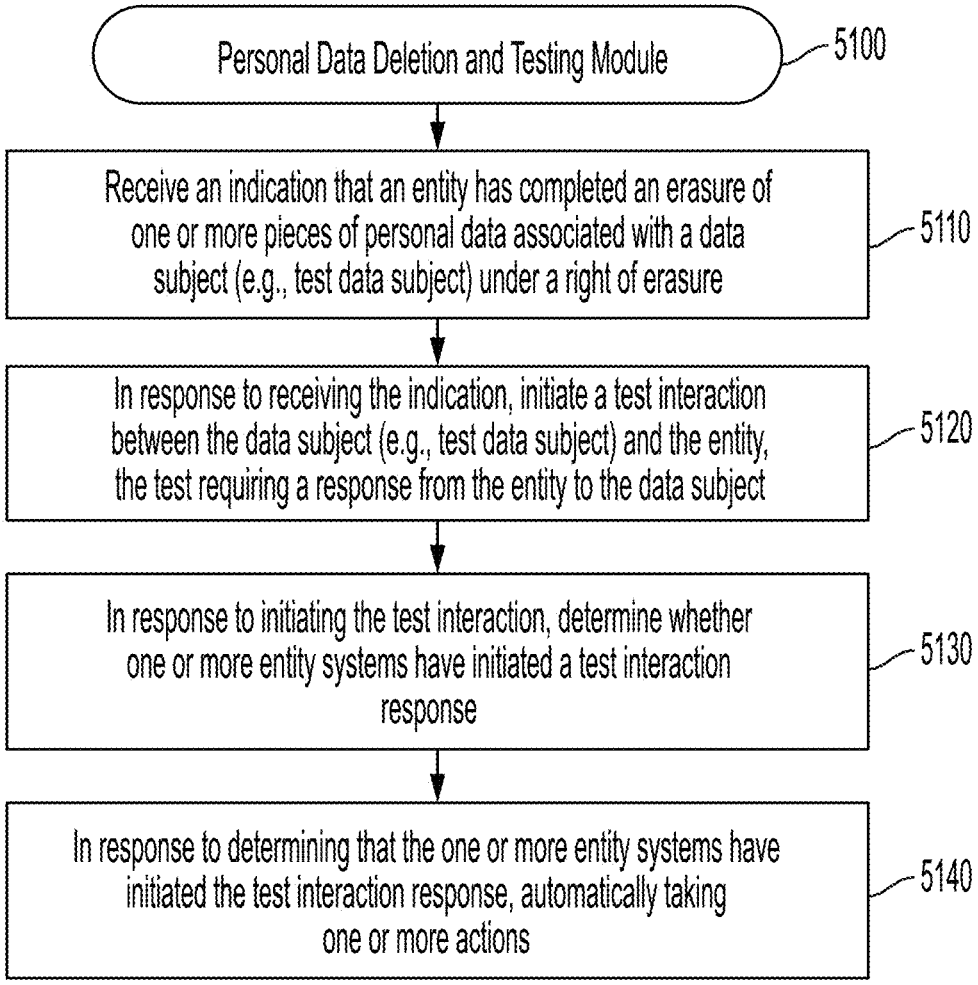

Personal Data Deletion and Testing Module
5100
Receive an indication that an entity has completed an erasure of one or more pieces of personal data associated with a data subject (e.g., test data subject) under a right of erasure
5110
In response to receiving the indication, initiate a test interaction between the data subject (e.g., test data subject) and the entity, the test requiring a response from the entity to the data subject
5120
In response to initiating the test interaction, determine whether one or more entity systems have initiated a test interaction response
5130
In response to determining that the one or more entity systems have initiated the test interaction response, automatically taking one or more actions
5140

FIG. 51

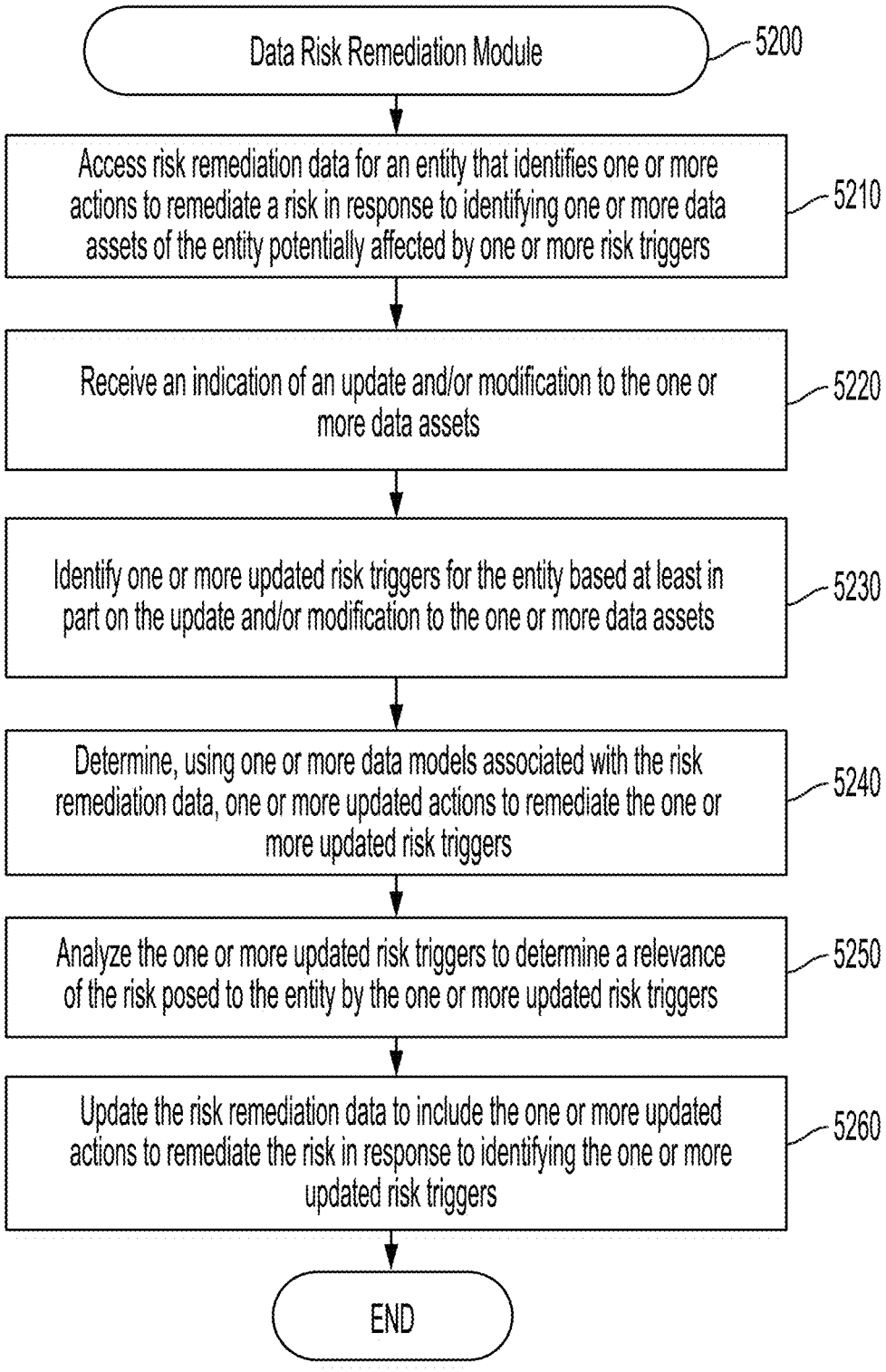

Data Risk Remediation Module
5200
Access risk remediation data for an entity that identifies one or more actions to remediate a risk in response to identifying one or more data assets of the entity potentially affected by one or more risk triggers
5210
Receive an indication of an update and/or modification to the one or more data assets
5220
Identify one or more updated risk triggers for the entity based at least in part on the update and/or modification to the one or more data assets
5230
Determine, using one or more data models associated with the risk remediation data, one or more updated actions to remediate the one or more updated risk triggers
5240
Analyze the one or more updated risk triggers to determine a relevance of the risk posed to the entity by the one or more updated risk triggers
5250
Update the risk remediation data to include the one or more updated actions to remediate the risk in response to identifying the one or more updated risk triggers
5260
END

FIG. 52

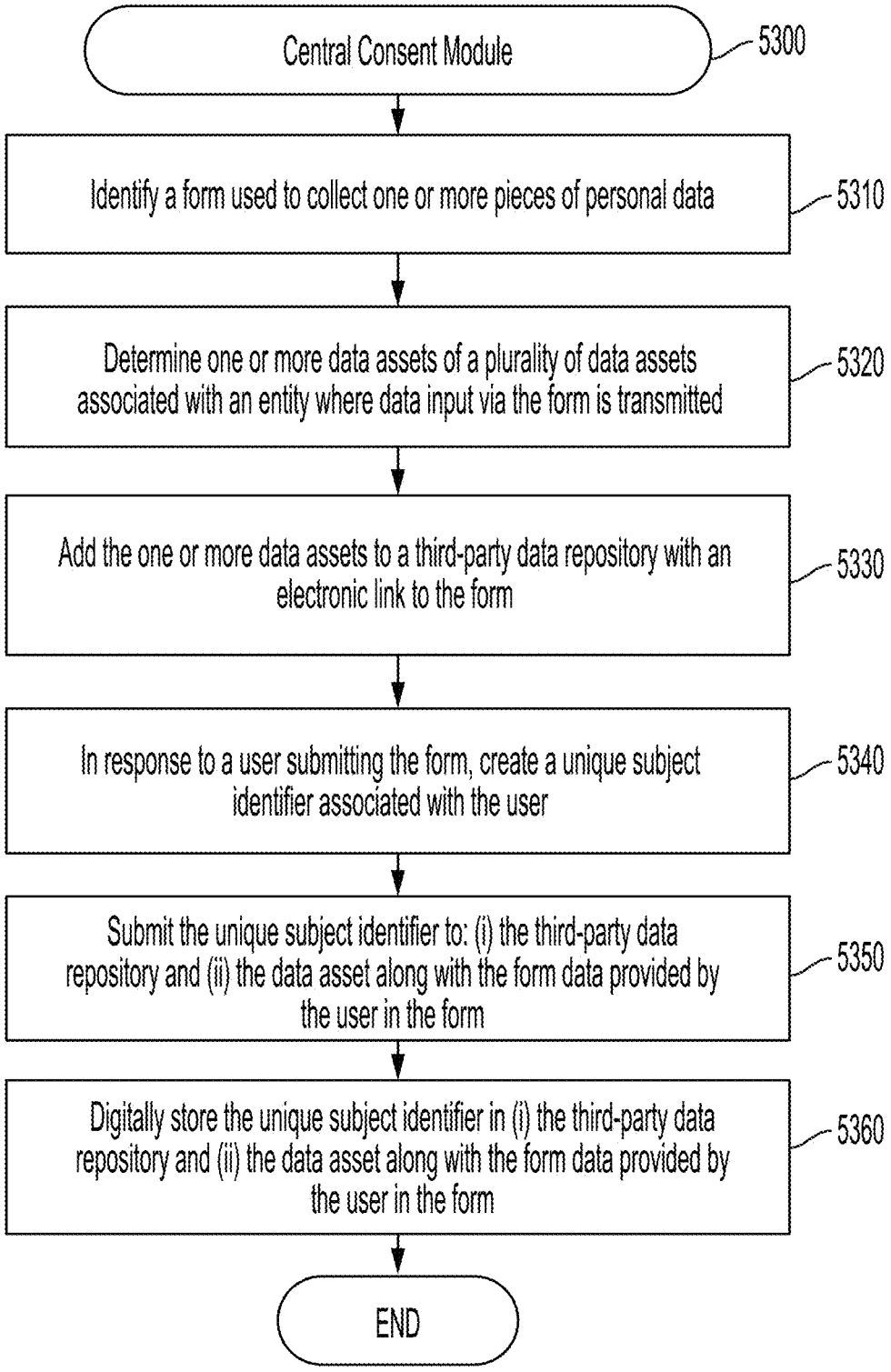

Central Consent Module
5300
Identify a form used to collect one or more pieces of personal data
5310
Determine one or more data assets of a plurality of data assets associated with an entity where data input via the form is transmitted
5320
Add the one or more data assets to a third-party data repository with an electronic link to the form
5330
In response to a user submitting the form, create a unique subject identifier associated with the user
5340
Submit the unique subject identifier to: (i) the third-party data repository and (ii) the data asset along with the form data provided by the user in the form
5350
Digitally store the unique subject identifier in (i) the third-party data repository and (ii) the data asset along with the form data provided by the user in the form
5360
END

FIG. 53

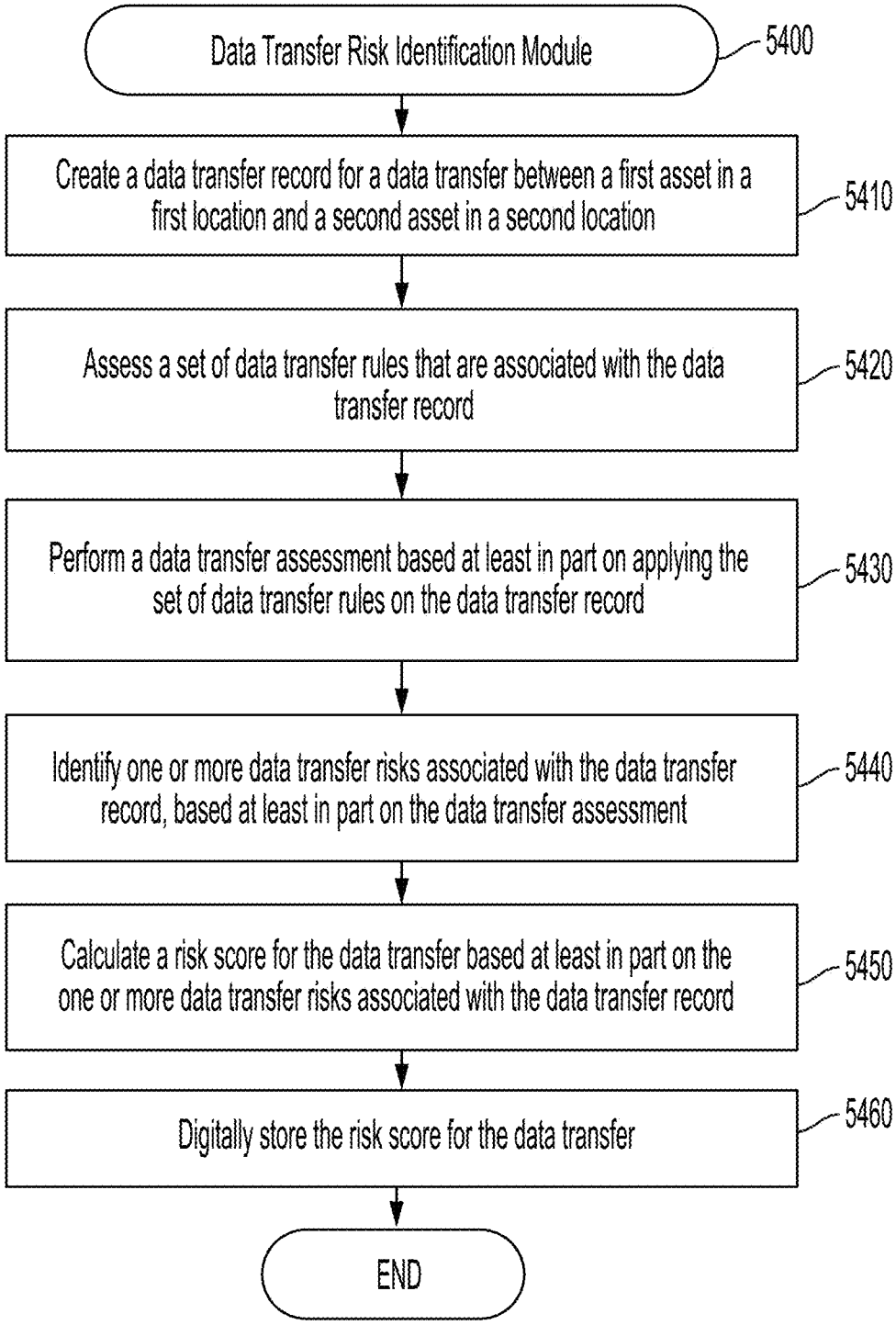

Data Transfer Risk Identification Module
5400
Create a data transfer record for a data transfer between a first asset in a first location and a second asset in a second location
5410
Assess a set of data transfer rules that are associated with the data transfer record
5420
Perform a data transfer assessment based at least in part on applying the set of data transfer rules on the data transfer record
5430
Identify one or more data transfer risks associated with the data transfer record, based at least in part on the data transfer assessment
5440
Calculate a risk score for the data transfer based at least in part on the one or more data transfer risks associated with the data transfer record
5450
Digitally store the risk score for the data transfer
5460
END

FIG. 54

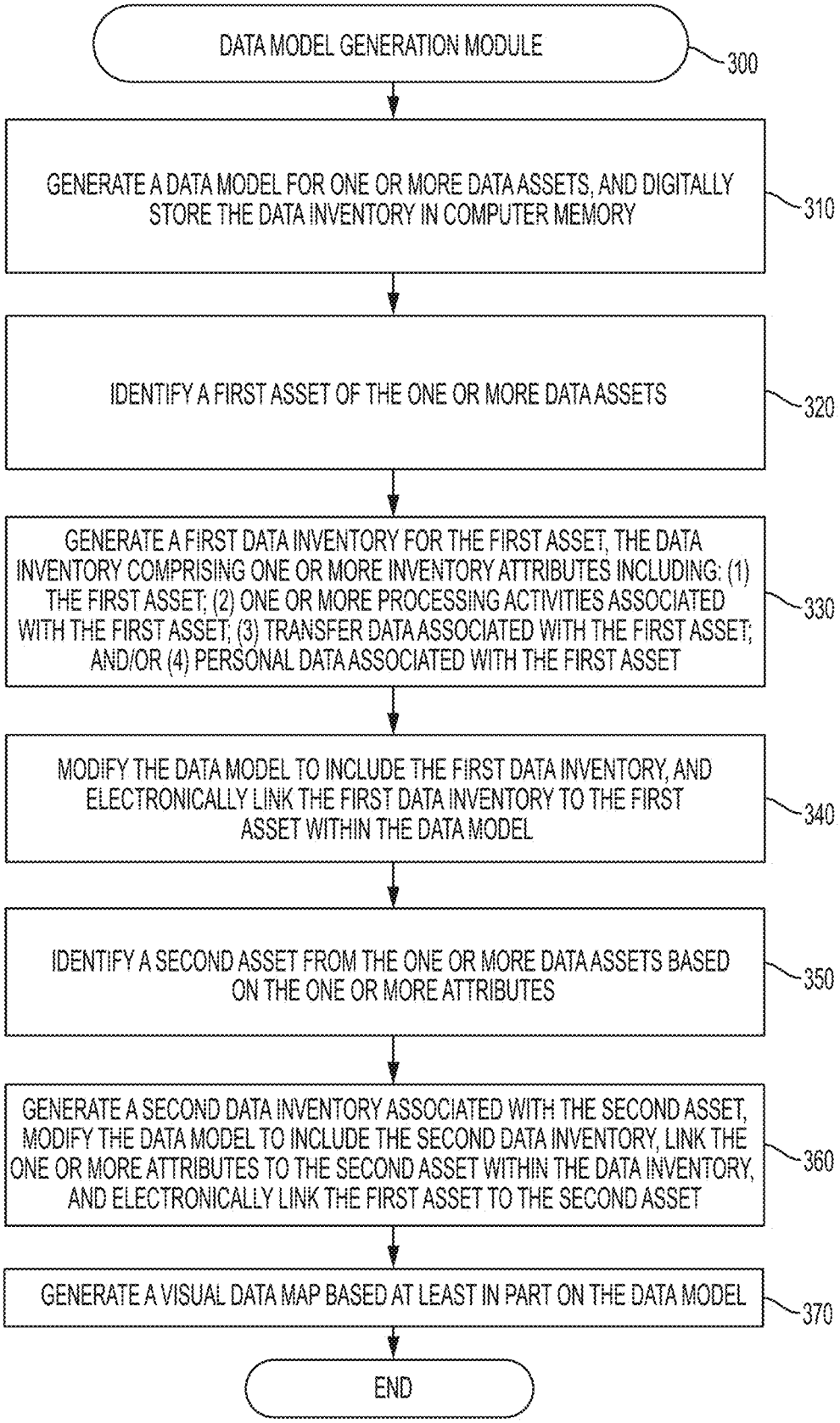

DATA MODEL GENERATION MODULE
300
GENERATE A DATA MODEL FOR ONE OR MORE DATA ASSETS, AND DIGITALLY STORE THE DATA INVENTORY IN COMPUTER MEMORY
310
IDENTIFY A FIRST ASSET OF THE ONE OR MORE DATA ASSETS
320
GENERATE A FIRST DATA INVENTORY FOR THE FIRST ASSET, THE DATA INVENTORY COMPRISING ONE OR MORE INVENTORY ATTRIBUTES INCLUDING: (1) THE FIRST ASSET; (2) ONE OR MORE PROCESSING ACTIVITIES ASSOCIATED WITH THE FIRST ASSET; (3) TRANSFER DATA ASSOCIATED WITH THE FIRST ASSET; AND/OR (4) PERSONAL DATA ASSOCIATED WITH THE FIRST ASSET
330
MODIFY THE DATA MODEL TO INCLUDE THE FIRST DATA INVENTORY, AND ELECTRONICALLY LINK THE FIRST DATA INVENTORY TO THE FIRST ASSET WITHIN THE DATA MODEL
340
IDENTIFY A SECOND ASSET FROM THE ONE OR MORE DATA ASSETS BASED ON THE ONE OR MORE ATTRIBUTES
350
GENERATE A SECOND DATA INVENTORY ASSOCIATED WITH THE SECOND ASSET, MODIFY THE DATA MODEL TO INCLUDE THE SECOND DATA INVENTORY, LINK THE ONE OR MORE ATTRIBUTES TO THE SECOND ASSET WITHIN THE DATA INVENTORY, AND ELECTRONICALLY LINK THE FIRST ASSET TO THE SECOND ASSET
360
GENERATE A VISUAL DATA MAP BASED AT LEAST IN PART ON THE DATA MODEL
370
END

FIG. 55

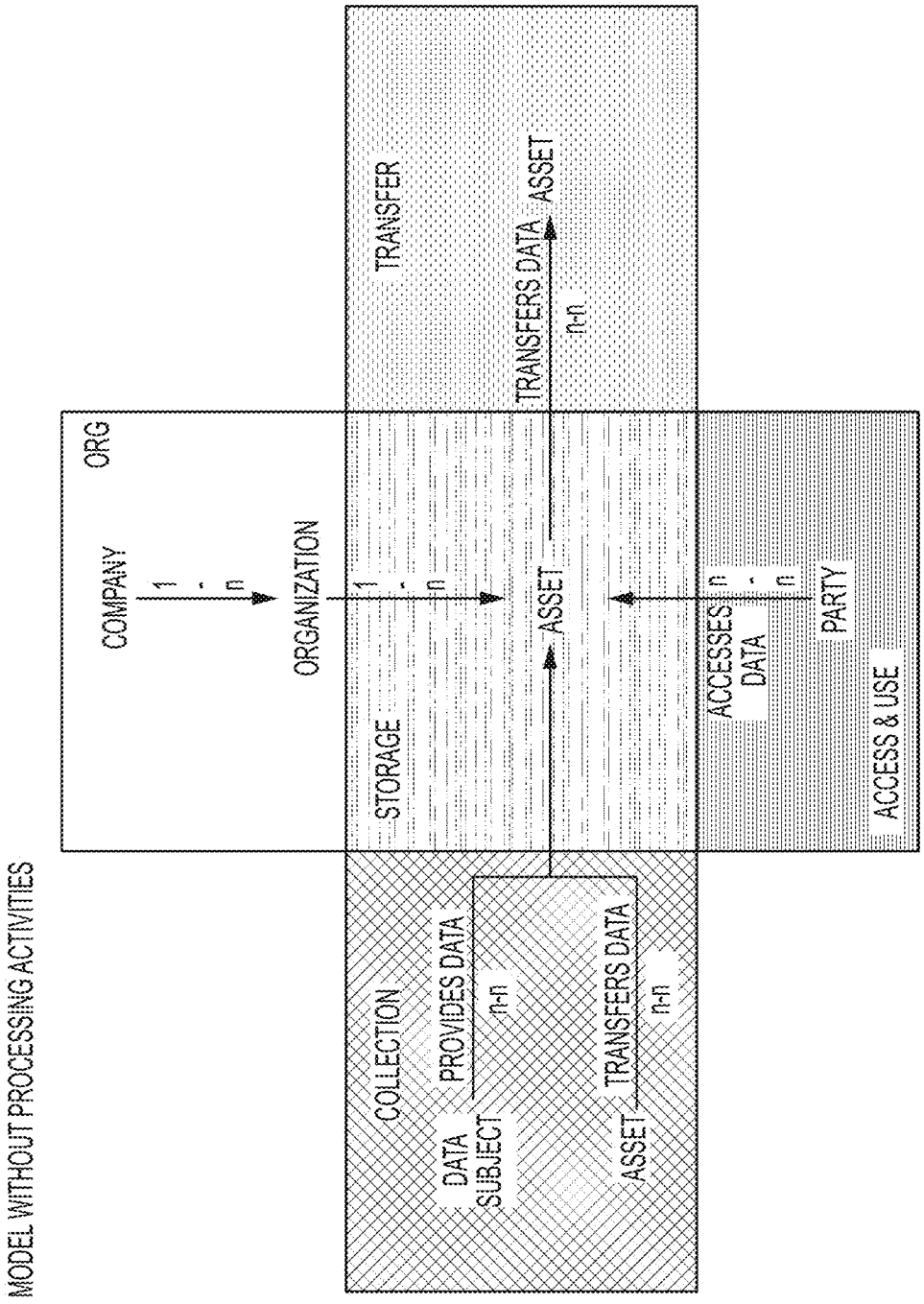

MODEL WITHOUT PROCESSING ACTIVITIES
ORG
COMPANY
1
-
n
ORGANIZATION
1
-
n
STORAGE
TRANSFER
TRANSFERS DATA
ASSET
n-n
ASSET
ACCESSES
DATA
n
-
n
PARTY
ACCESS & USE
COLLECTION
DATA SUBJECT
PROVIDES DATA
n-n
ASSET
TRANSFERS DATA
n-n

FIG. 56

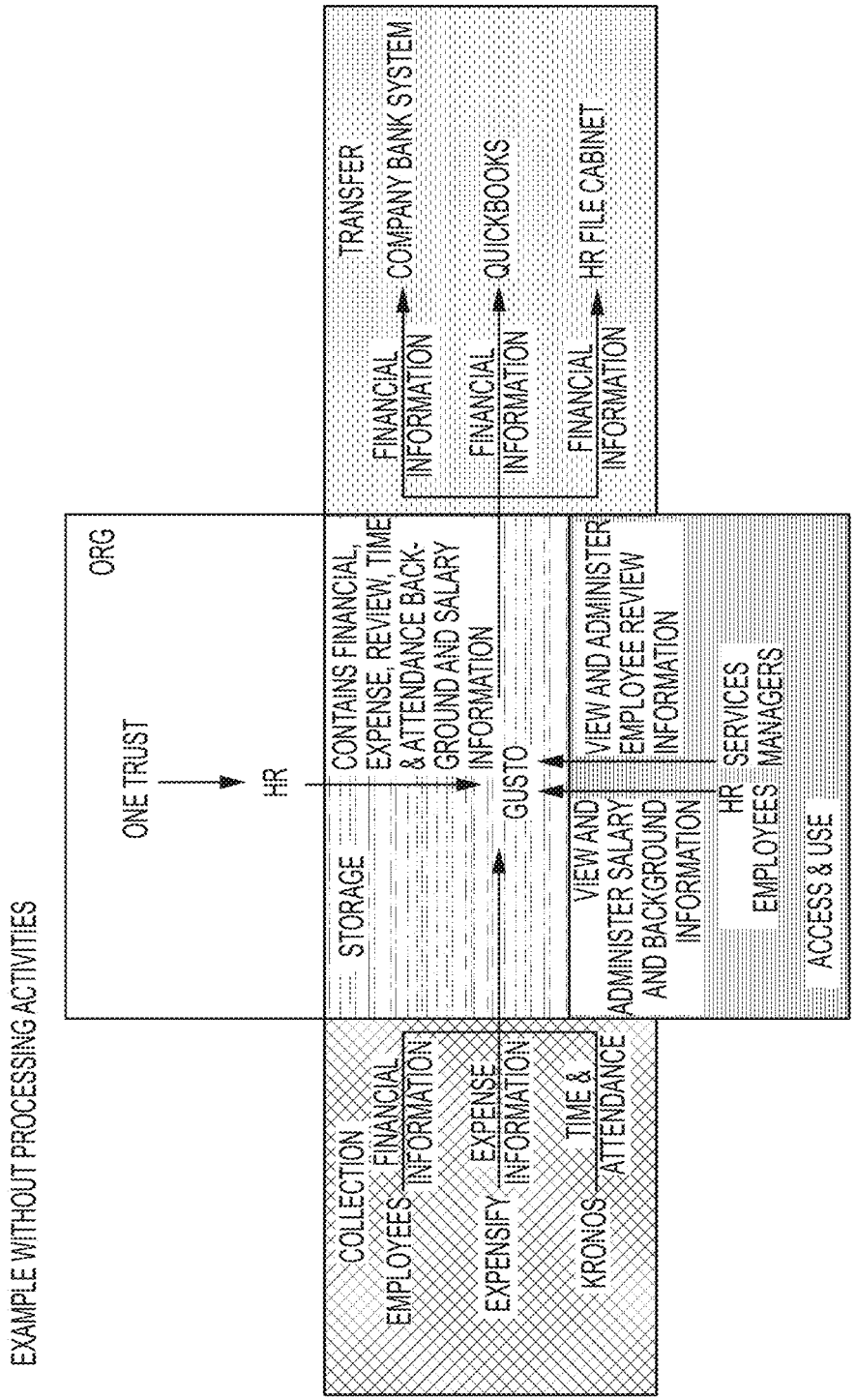

EXAMPLE WITHOUT PROCESSING ACTIVITIES
ORG
ONE TRUST
HR
STORAGE
CONTAINS FINANCIAL, EXPENSE, REVIEW, TIME & ATTENDANCE BACK-GROUND AND SALARY INFORMATION
GUSTO
VIEW AND ADMINISTER SALARY AND BACKGROUND INFORMATION
VIEW AND ADMINISTER EMPLOYEE REVIEW INFORMATION
HR SERVICES EMPLOYEES MANAGERS
ACCESS & USE
TRANSFER
FINANCIAL INFORMATION
COMPANY BANK SYSTEM
FINANCIAL INFORMATION
QUICKBOOKS
FINANCIAL INFORMATION
HR FILE CABINET
COLLECTION
EMPLOYEES FINANCIAL INFORMATION
EXPENSIFY EXPENSE INFORMATION
KRONOS TIME & ATTENDANCE

FIG. 57

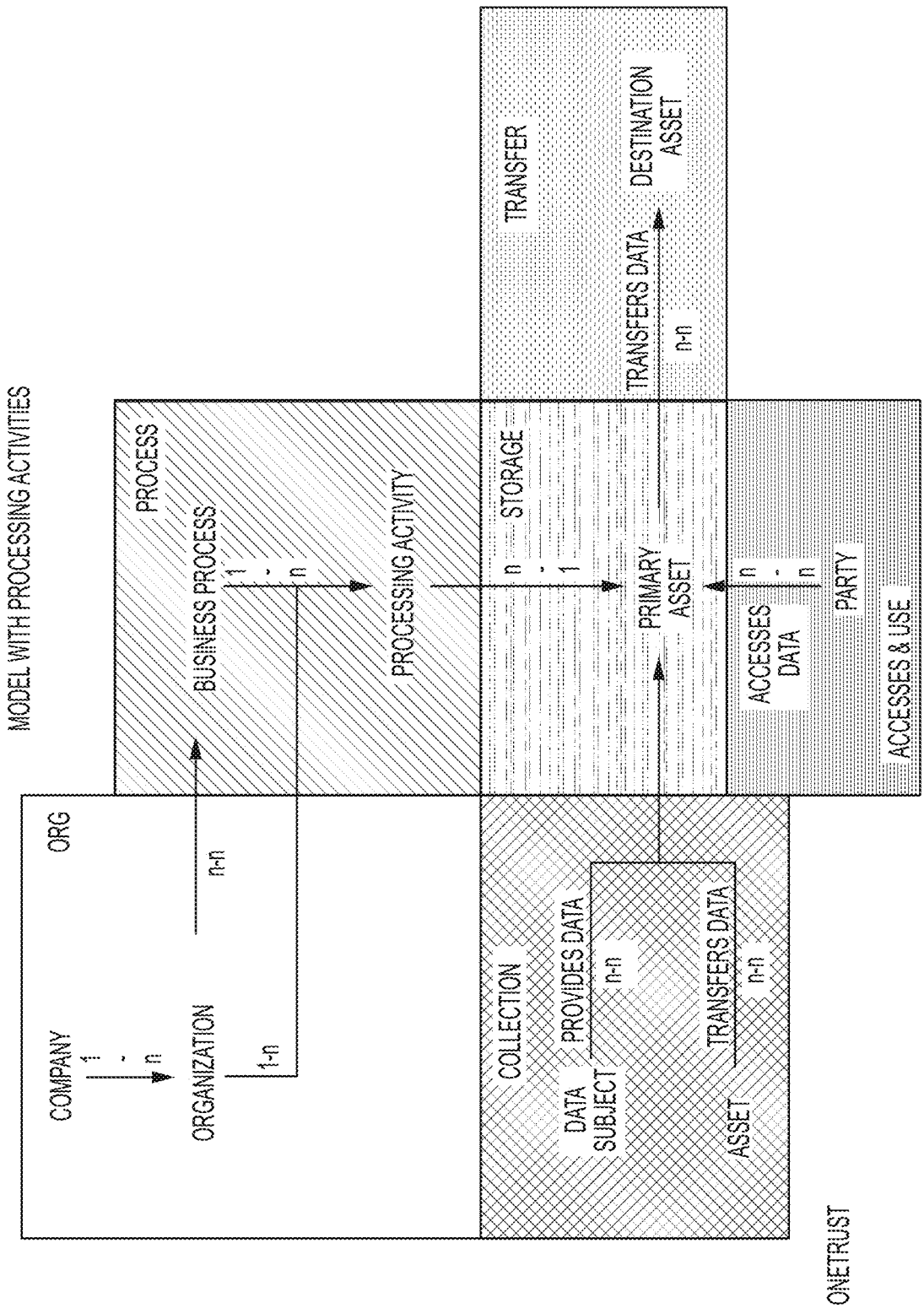

MODEL WITH PROCESSING ACTIVITIES
ORG
COMPANY
1
-
n
ORGANIZATION
n-n
1-n
PROCESS
BUSINESS PROCESS
1
-
n
PROCESSING ACTIVITY
COLLECTION
DATA SUBJECT
PROVIDES DATA
n-n
ASSET
TRANSFERS DATA
n-n
STORAGE
n
-
1
TRANSFER
TRANSFERS DATA
n-n
PRIMARY ASSET
DESTINATION ASSET
ACCESSES DATA
n
-
n
PARTY
ACCESSES & USE
ONETRUST

FIG. 58

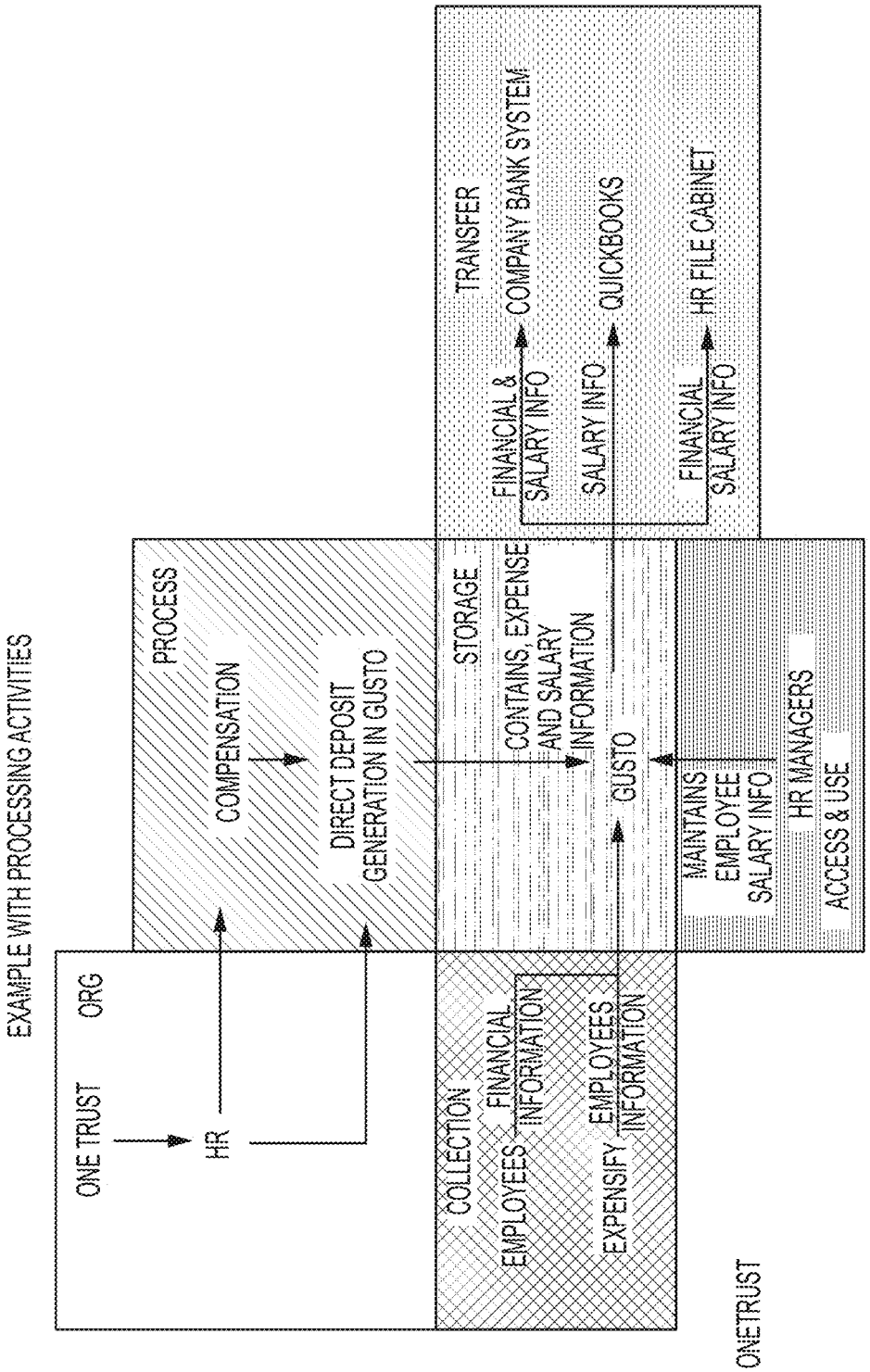

EXAMPLE WITH PROCESSING ACTIVITIES
ONE TRUST ORG
HR
PROCESS
COMPENSATION
DIRECT DEPOSIT GENERATION IN GUSTO
STORAGE
CONTAINS, EXPENSE AND SALARY INFORMATION
GUSTO
TRANSFER
FINANCIAL & SALARY INFO
COMPANY BANK SYSTEM
SALARY INFO
QUICKBOOKS
FINANCIAL SALARY INFO
HR FILE CABINET
COLLECTION
EMPLOYEES FINANCIAL INFORMATION
EXPENSIFY EMPLOYEES INFORMATION
MAINTAINS EMPLOYEE SALARY INFO
HR MANAGERS
ACCESS & USE
ONETRUST

FIG. 59

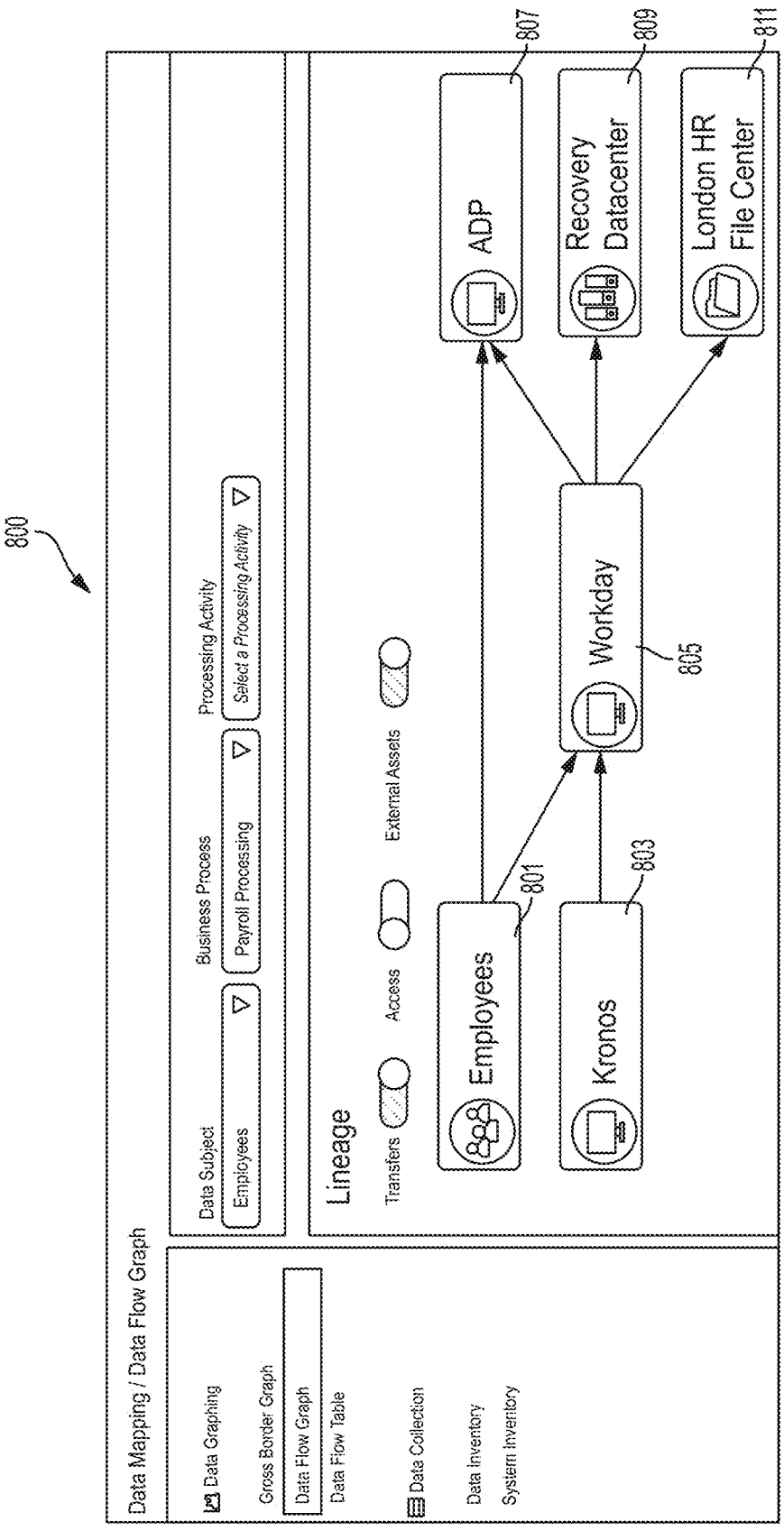

800
Data Mapping / Data Flow Graph
Data Graphing
Gross Border Graph
Data Flow Graph
Data Flow Table
Data Collection
Data Inventory
System Inventory
Data Subject
Employees
Business Process
Payroll Processing
Processing Activity
Select a Processing Activity
Lineage
Transfers
Access
External Assets
Employees
801
Kronos
803
Workday
805
ADP
807
Recovery Datacenter
809
London HR File Center
811

FIG. 60

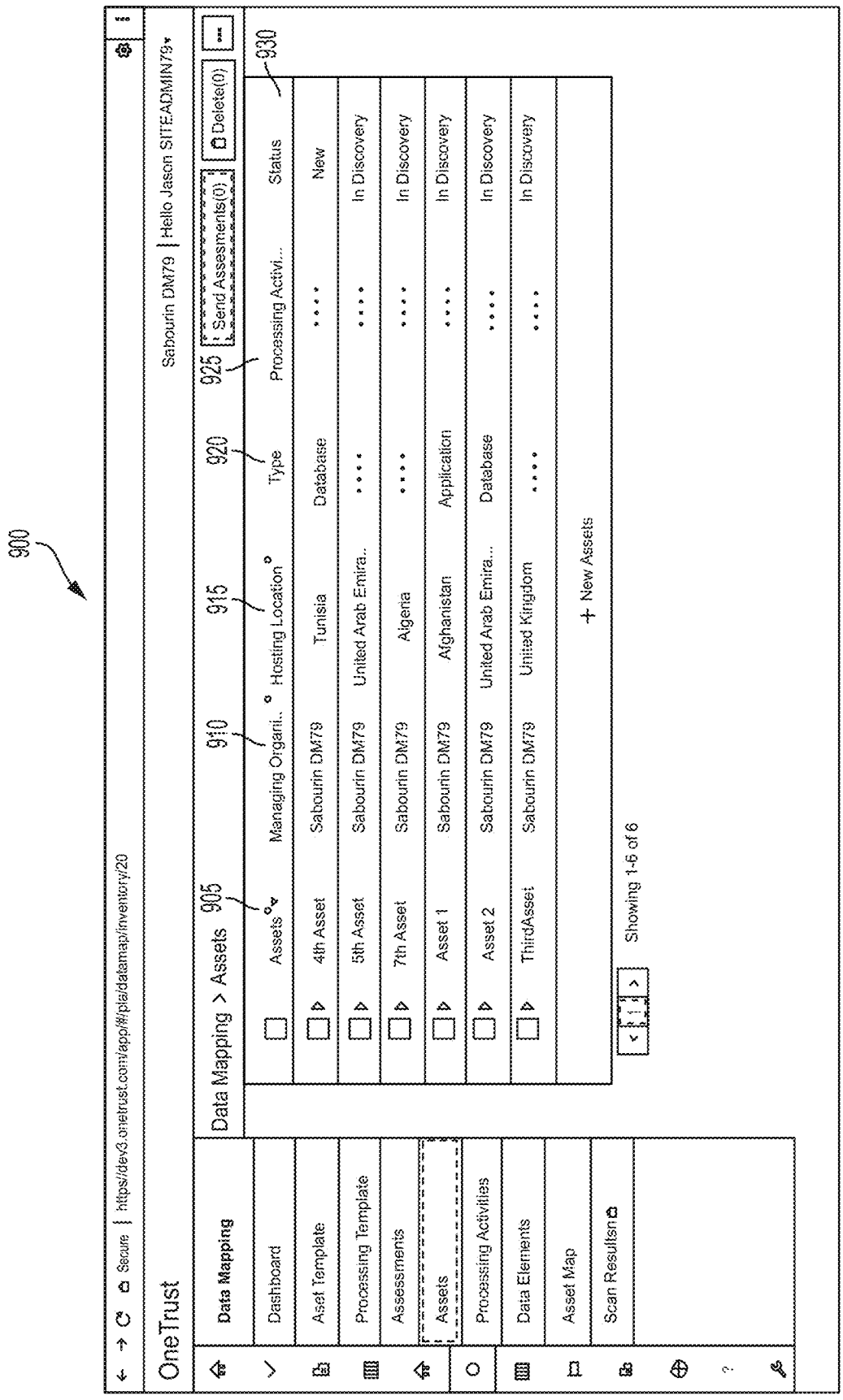

900
OneTrust
Secure | https://dev3.onetrust.com/app/#/pia/datamap/inventory/20
Sabourin DM79 | Hello Jason SITEADMIN79
Data Mapping
Dashboard
Asset Template
Processing Template
Assessments
Assets
Processing Activities
Data Elements
Asset Map
Scan Results
Data Mapping > Assets
905
910
915
920
925
930
Send Assesments(0)
Delete(0)
Assets
Managing Organi...
Hosting Location
Type
Processing Activi...
Status
4th Asset
Sabourin DM79
Tunisia
Database
New
5th Asset
Sabourin DM79
United Arab Emira...
In Discovery
7th Asset
Sabourin DM79
Algeria
In Discovery
Asset 1
Sabourin DM79
Afghanistan
Application
In Discovery
Asset 2
Sabourin DM79
United Arab Emira...
Database
In Discovery
ThirdAsset
Sabourin DM79
United Kingdom
In Discovery
+ New Assets
Showing 1-6 of 6

FIG. 61

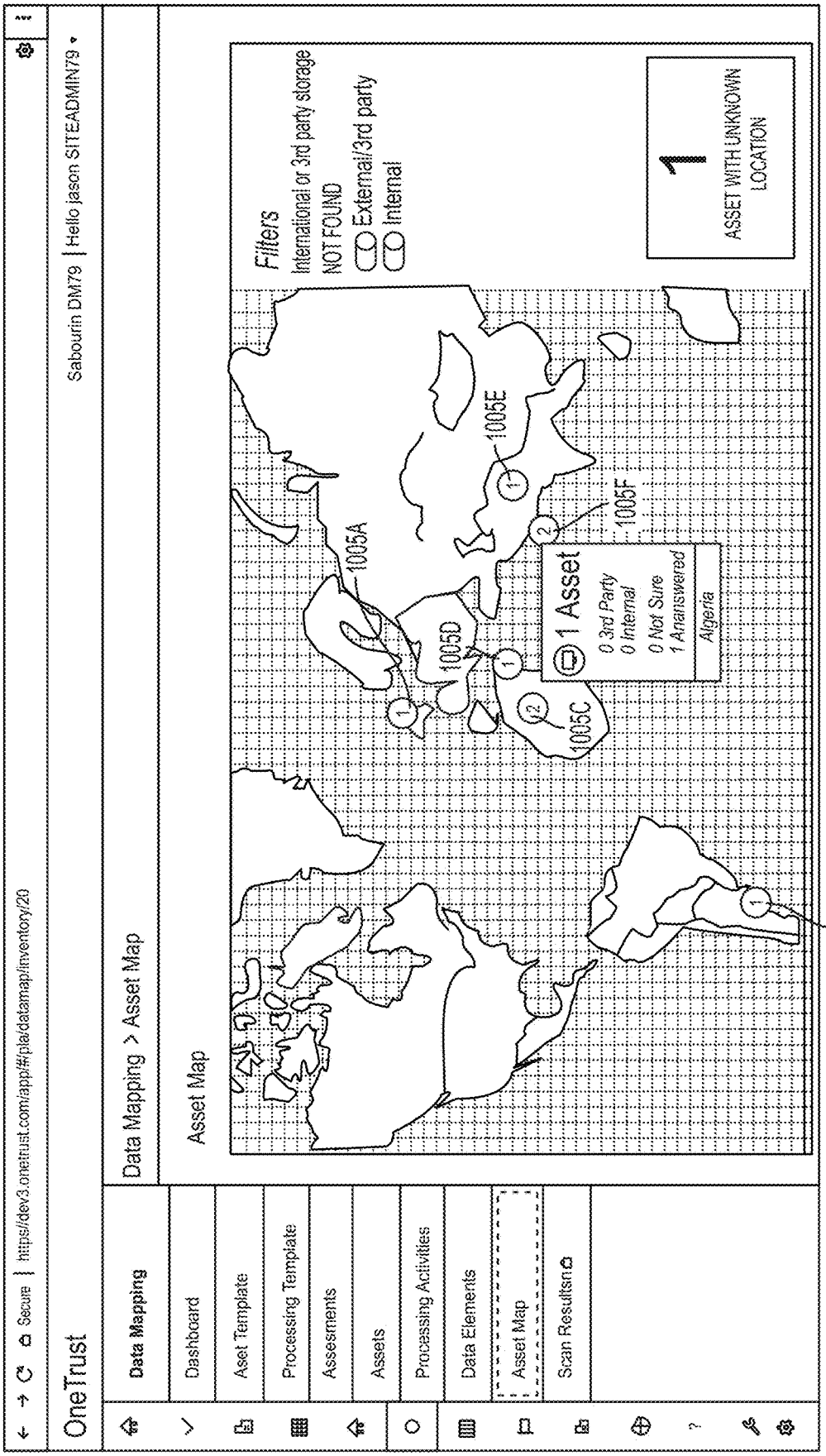

OneTrust
Secure | https://dev3.onetrust.com/app/#/pia/datamap/inventory/20
Sabourin DM79 | Hello jason SITEADMIN79
Data Mapping
Dashboard
Aset Template
Processing Template
Assesments
Assets
Processing Activities
Data Elements
Asset Map
Scan Results
Data Mapping > Asset Map
Asset Map
Filters
International or 3rd party storage
NOT FOUND
External/3rd party
Internal
1005A
1005B
1005C
1005D
1005E
1005F
1 Asset
0 3rd Party
0 Internal
0 Not Sure
1 Anaswered
Algeria
1
ASSET WITH UNKNOWN LOCATION

FIG. 62

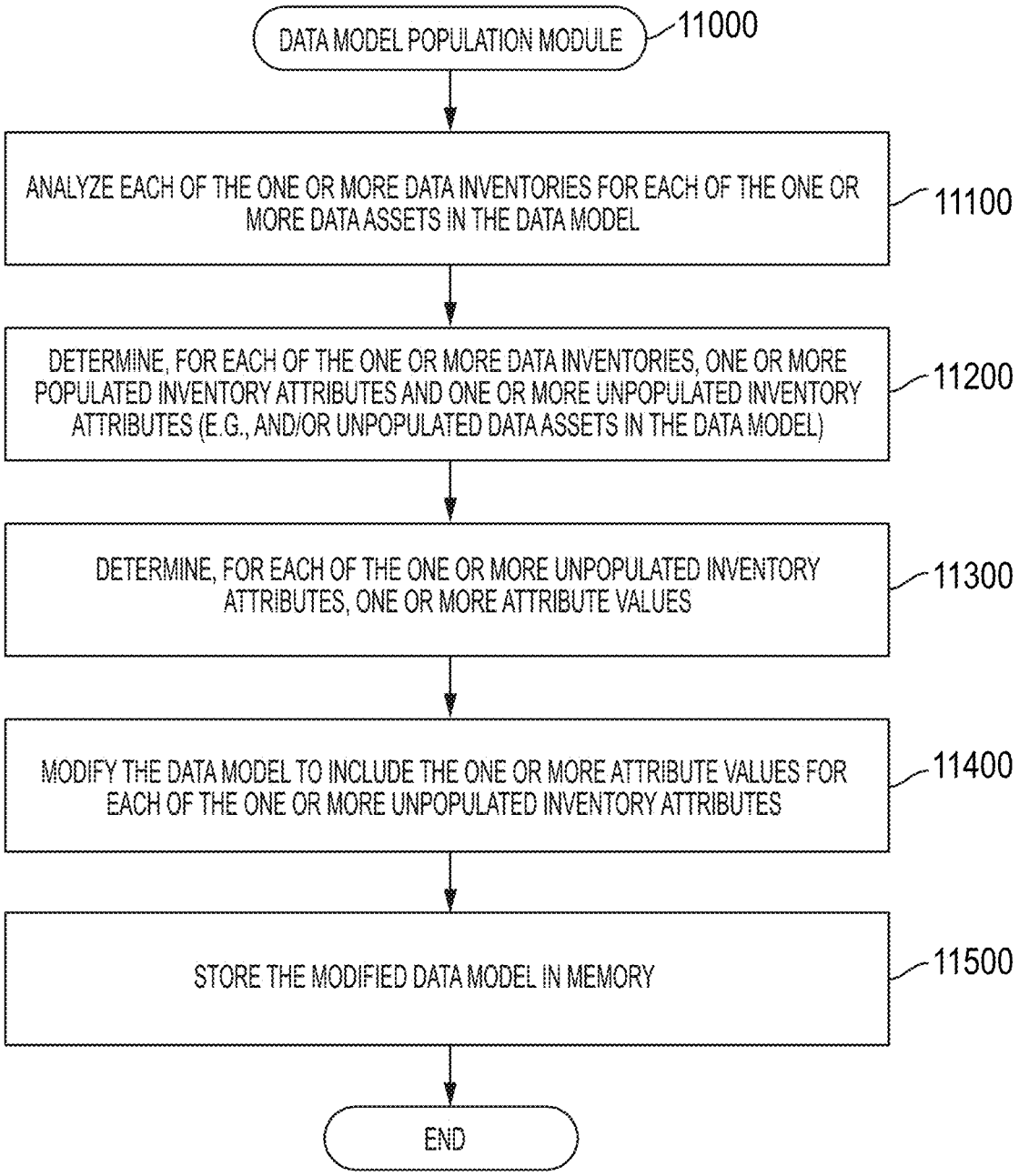

DATA MODEL POPULATION MODULE
11000
ANALYZE EACH OF THE ONE OR MORE DATA INVENTORIES FOR EACH OF THE ONE OR MORE DATA ASSETS IN THE DATA MODEL
11100
DETERMINE, FOR EACH OF THE ONE OR MORE DATA INVENTORIES, ONE OR MORE POPULATED INVENTORY ATTRIBUTES AND ONE OR MORE UNPOPULATED INVENTORY ATTRIBUTES (E.G., AND/OR UNPOPULATED DATA ASSETS IN THE DATA MODEL)
11200
DETERMINE, FOR EACH OF THE ONE OR MORE UNPOPULATED INVENTORY ATTRIBUTES, ONE OR MORE ATTRIBUTE VALUES
11300
MODIFY THE DATA MODEL TO INCLUDE THE ONE OR MORE ATTRIBUTE VALUES FOR EACH OF THE ONE OR MORE UNPOPULATED INVENTORY ATTRIBUTES
11400
STORE THE MODIFIED DATA MODEL IN MEMORY
11500
END

FIG. 63

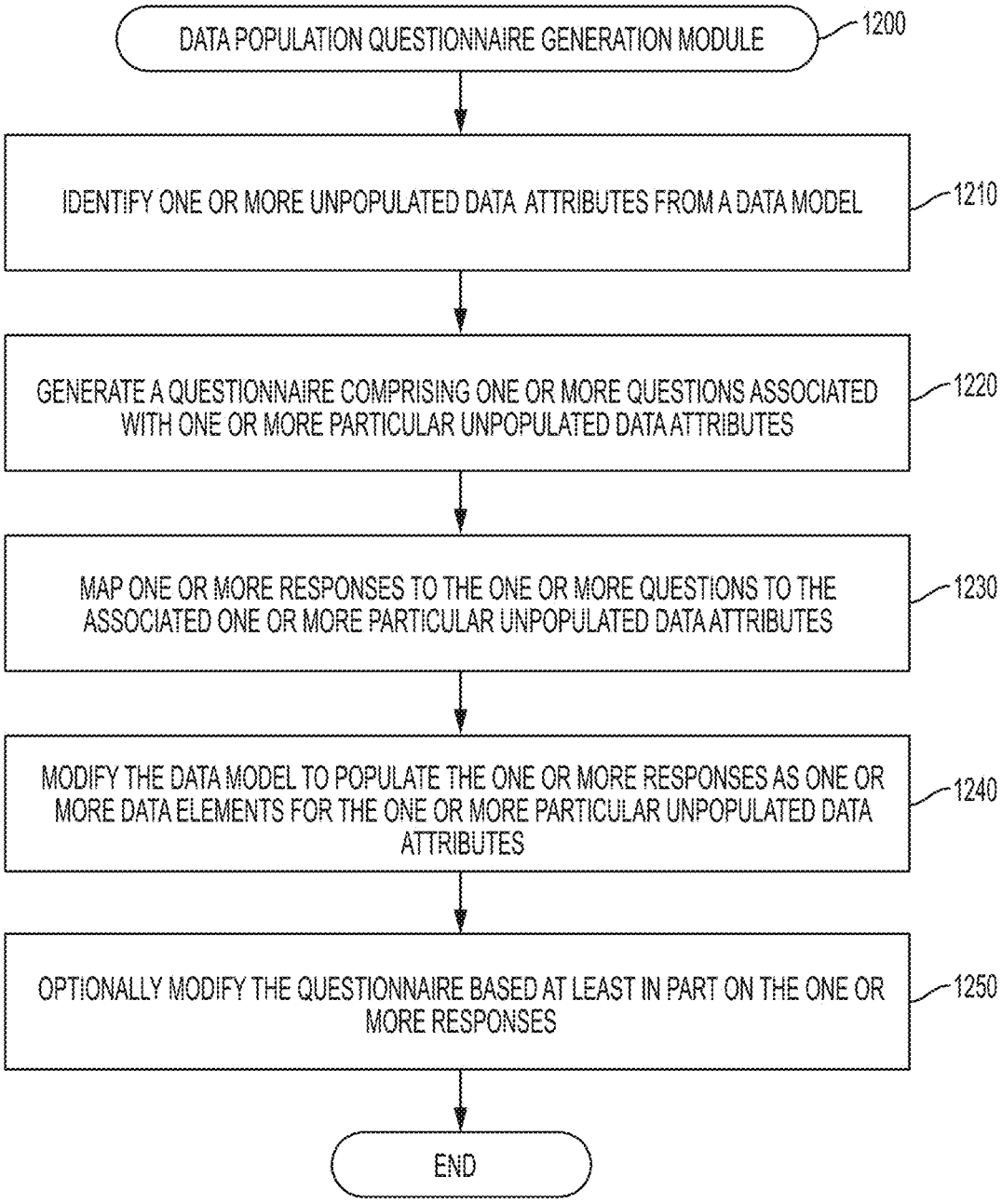

DATA POPULATION QUESTIONNAIRE GENERATION MODULE
1200
IDENTIFY ONE OR MORE UNPOPULATED DATA ATTRIBUTES FROM A DATA MODEL
1210
GENERATE A QUESTIONNAIRE COMPRISING ONE OR MORE QUESTIONS ASSOCIATED WITH ONE OR MORE PARTICULAR UNPOPULATED DATA ATTRIBUTES
1220
MAP ONE OR MORE RESPONSES TO THE ONE OR MORE QUESTIONS TO THE ASSOCIATED ONE OR MORE PARTICULAR UNPOPULATED DATA ATTRIBUTES
1230
MODIFY THE DATA MODEL TO POPULATE THE ONE OR MORE RESPONSES AS ONE OR MORE DATA ELEMENTS FOR THE ONE OR MORE PARTICULAR UNPOPULATED DATA ATTRIBUTES
1240
OPTIONALLY MODIFY THE QUESTIONNAIRE BASED AT LEAST IN PART ON THE ONE OR MORE RESPONSES
1250
END

FIG. 64

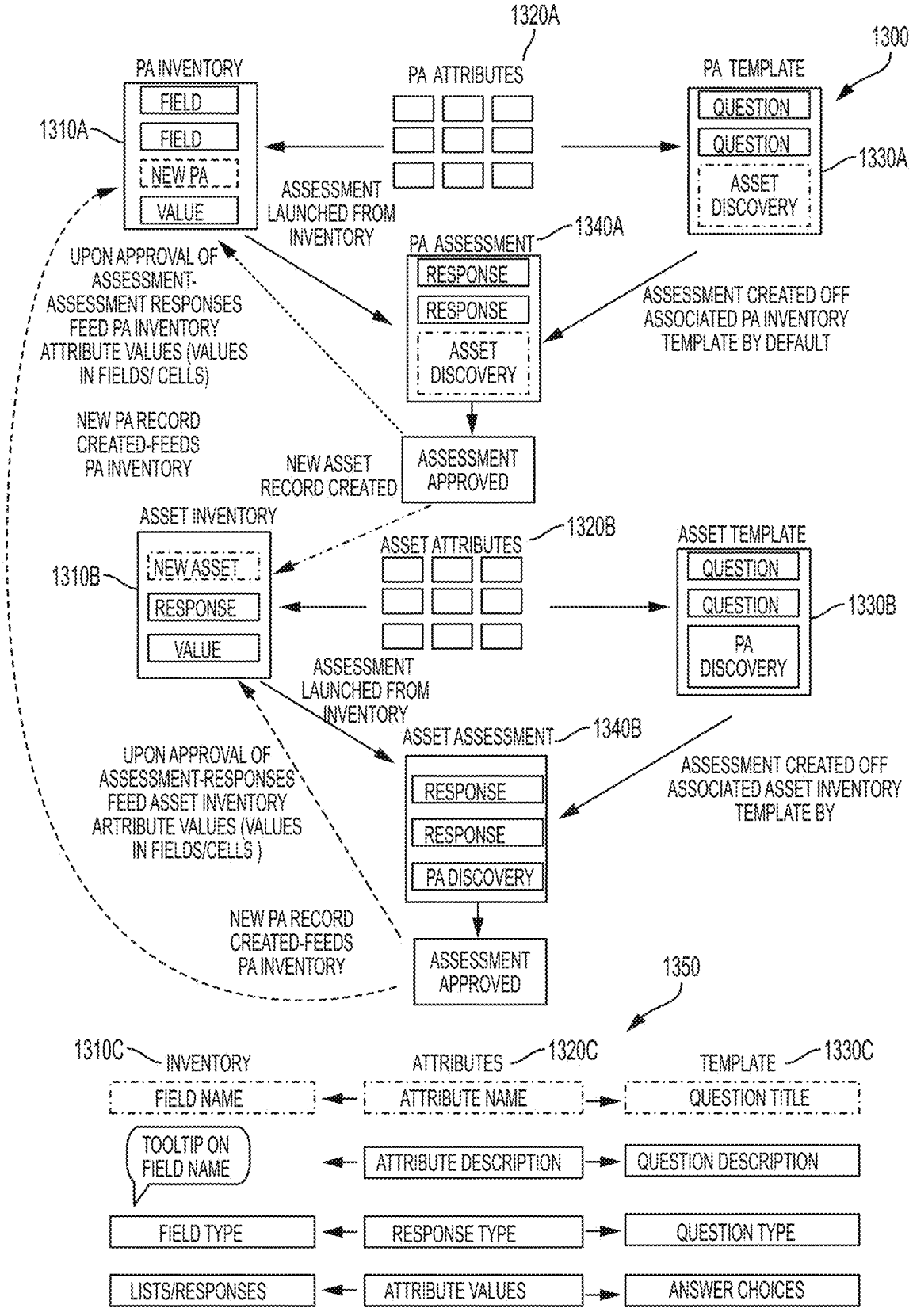

1320A
1300
PA INVENTORY
PA ATTRIBUTES
PA TEMPLATE
FIELD
FIELD
NEW PA
VALUE
1310A
QUESTION
QUESTION
ASSET DISCOVERY
1330A
ASSESSMENT LAUNCHED FROM INVENTORY
PA ASSESSMENT
1340A
RESPONSE
RESPONSE
ASSET DISCOVERY
UPON APPROVAL OF ASSESSMENT- ASSESSMENT RESPONSES FEED PA INVENTORY ATTRIBUTE VALUES (VALUES IN FIELDS/ CELLS)
ASSESSMENT CREATED OFF ASSOCIATED PA INVENTORY TEMPLATE BY DEFAULT
NEW PA RECORD CREATED-FEEDS PA INVENTORY
NEW ASSET RECORD CREATED
ASSESSMENT APPROVED
ASSET INVENTORY
ASSET ATTRIBUTES
1320B
ASSET TEMPLATE
1310B
NEW ASSET
RESPONSE
VALUE
QUESTION
QUESTION
PA DISCOVERY
1330B
ASSESSMENT LAUNCHED FROM INVENTORY
ASSET ASSESSMENT
1340B
RESPONSE
RESPONSE
PA DISCOVERY
UPON APPROVAL OF ASSESSMENT-RESPONSES FEED ASSET INVENTORY ARTRIBUTE VALUES (VALUES IN FIELDS/CELLS)
ASSESSMENT CREATED OFF ASSOCIATED ASSET INVENTORY TEMPLATE BY
NEW PA RECORD CREATED-FEEDS PA INVENTORY
ASSESSMENT APPROVED
1350
1310C
INVENTORY
ATTRIBUTES
1320C
TEMPLATE
1330C
FIELD NAME
ATTRIBUTE NAME
QUESTION TITLE
TOOLTIP ON FIELD NAME
ATTRIBUTE DESCRIPTION
QUESTION DESCRIPTION
FIELD TYPE
RESPONSE TYPE
QUESTION TYPE
LISTS/RESPONSES
ATTRIBUTE VALUES
ANSWER CHOICES

FIG. 65

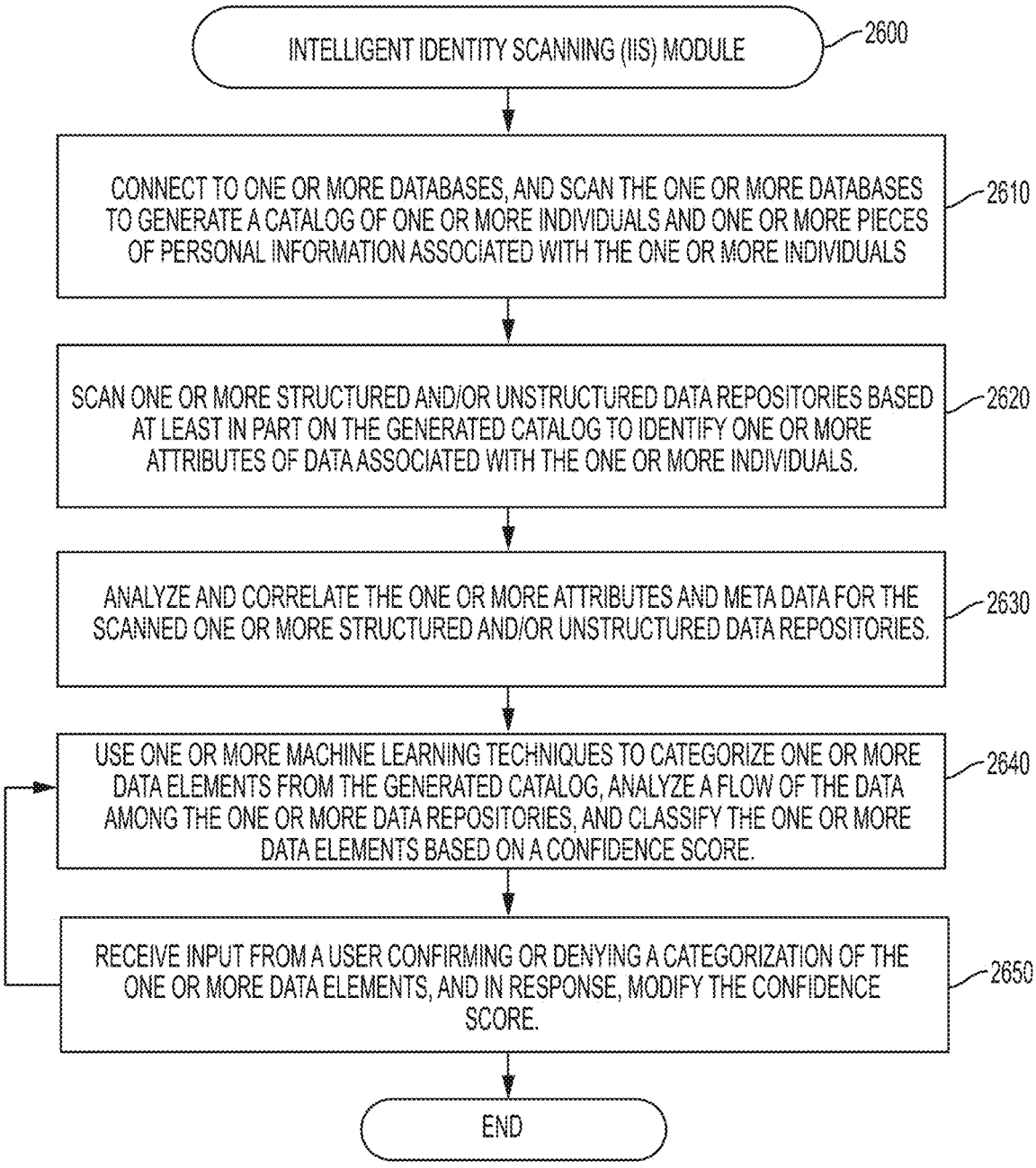

INTELLIGENT IDENTITY SCANNING (IIS) MODULE
2600
CONNECT TO ONE OR MORE DATABASES, AND SCAN THE ONE OR MORE DATABASES TO GENERATE A CATALOG OF ONE OR MORE INDIVIDUALS AND ONE OR MORE PIECES OF PERSONAL INFORMATION ASSOCIATED WITH THE ONE OR MORE INDIVIDUALS
2610
SCAN ONE OR MORE STRUCTURED AND/OR UNSTRUCTURED DATA REPOSITORIES BASED AT LEAST IN PART ON THE GENERATED CATALOG TO IDENTIFY ONE OR MORE ATTRIBUTES OF DATA ASSOCIATED WITH THE ONE OR MORE INDIVIDUALS.
2620
ANALYZE AND CORRELATE THE ONE OR MORE ATTRIBUTES AND META DATA FOR THE SCANNED ONE OR MORE STRUCTURED AND/OR UNSTRUCTURED DATA REPOSITORIES.
2630
USE ONE OR MORE MACHINE LEARNING TECHNIQUES TO CATEGORIZE ONE OR MORE DATA ELEMENTS FROM THE GENERATED CATALOG, ANALYZE A FLOW OF THE DATA AMONG THE ONE OR MORE DATA REPOSITORIES, AND CLASSIFY THE ONE OR MORE DATA ELEMENTS BASED ON A CONFIDENCE SCORE.
2640
RECEIVE INPUT FROM A USER CONFIRMING OR DENYING A CATEGORIZATION OF THE ONE OR MORE DATA ELEMENTS, AND IN RESPONSE, MODIFY THE CONFIDENCE SCORE.
2650
END

FIG. 66

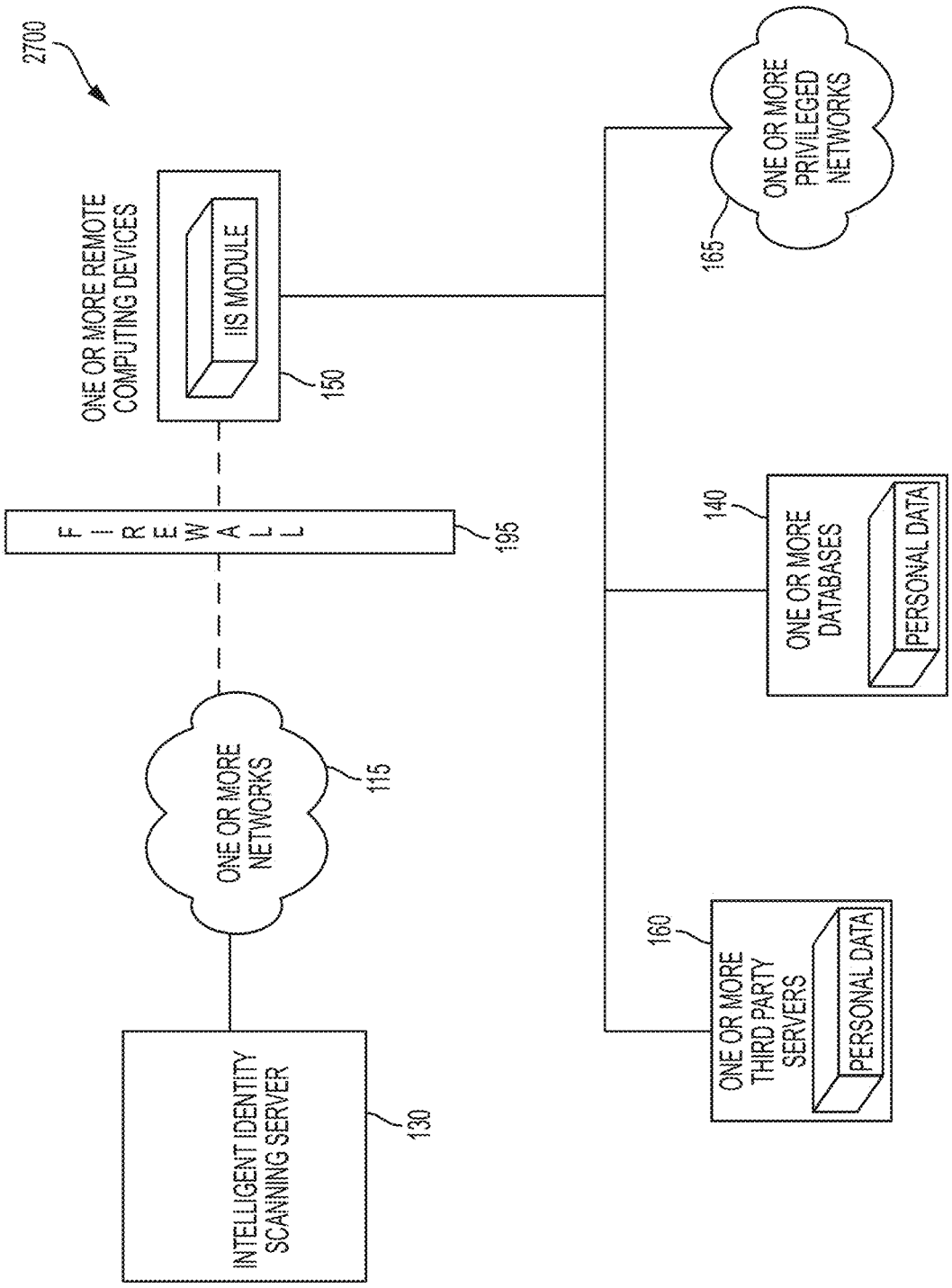

2700
ONE OR MORE REMOTE COMPUTING DEVICES
IIS MODULE
150
FIREWALL
195
ONE OR MORE NETWORKS
115
INTELLIGENT IDENTITY SCANNING SERVER
130
ONE OR MORE PRIVILEGED NETWORKS
165
ONE OR MORE DATABASES
140
PERSONAL DATA
ONE OR MORE THIRD PARTY SERVERS
160
PERSONAL DATA

FIG. 67

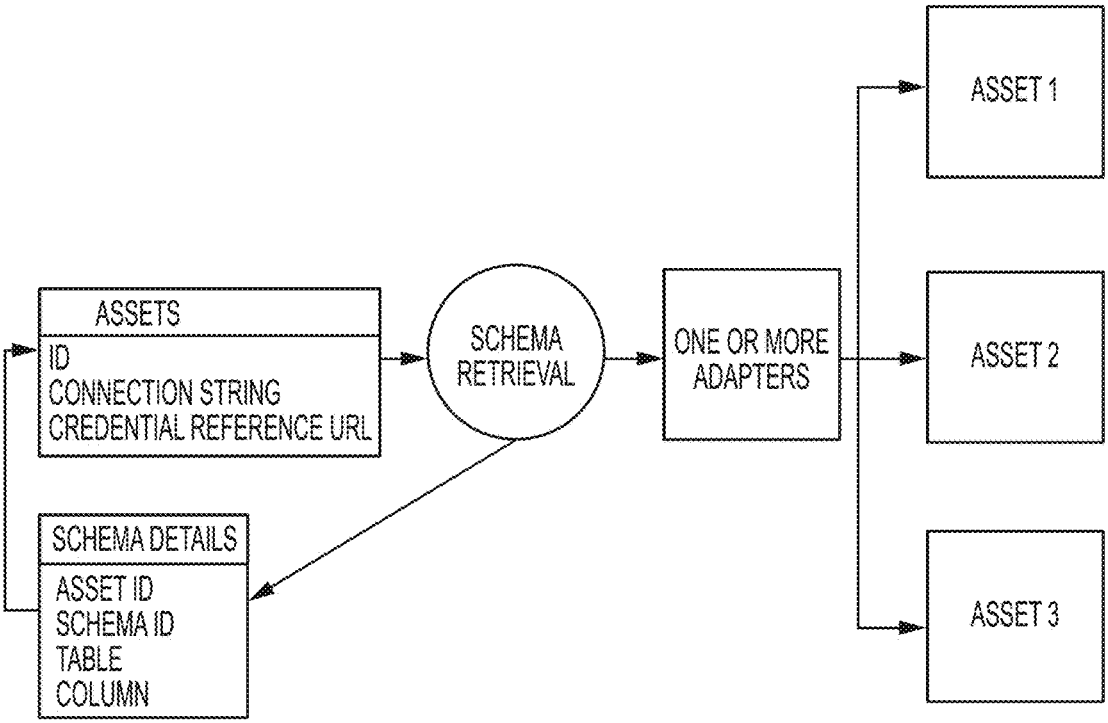

ASSETS
ID
CONNECTION STRING
CREDENTIAL REFERENCE URL
SCHEMA RETRIEVAL
ONE OR MORE ADAPTERS
ASSET 1
ASSET 2
ASSET 3
SCHEMA DETAILS
ASSET ID
SCHEMA ID
TABLE
COLUMN

FIG. 68

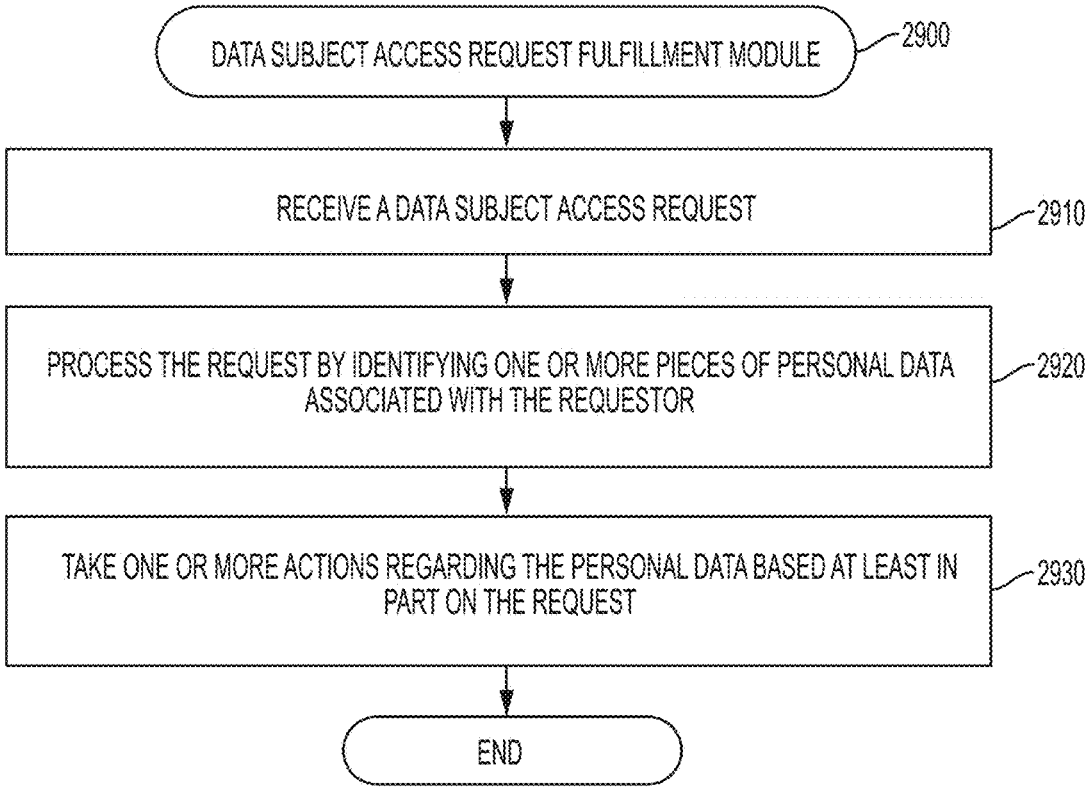

DATA SUBJECT ACCESS REQUEST FULFILLMENT MODULE
2900
RECEIVE A DATA SUBJECT ACCESS REQUEST
2910
PROCESS THE REQUEST BY IDENTIFYING ONE OR MORE PIECES OF PERSONAL DATA ASSOCIATED WITH THE REQUESTOR
2920
TAKE ONE OR MORE ACTIONS REGARDING THE PERSONAL DATA BASED AT LEAST IN PART ON THE REQUEST
2930
END

FIG. 69

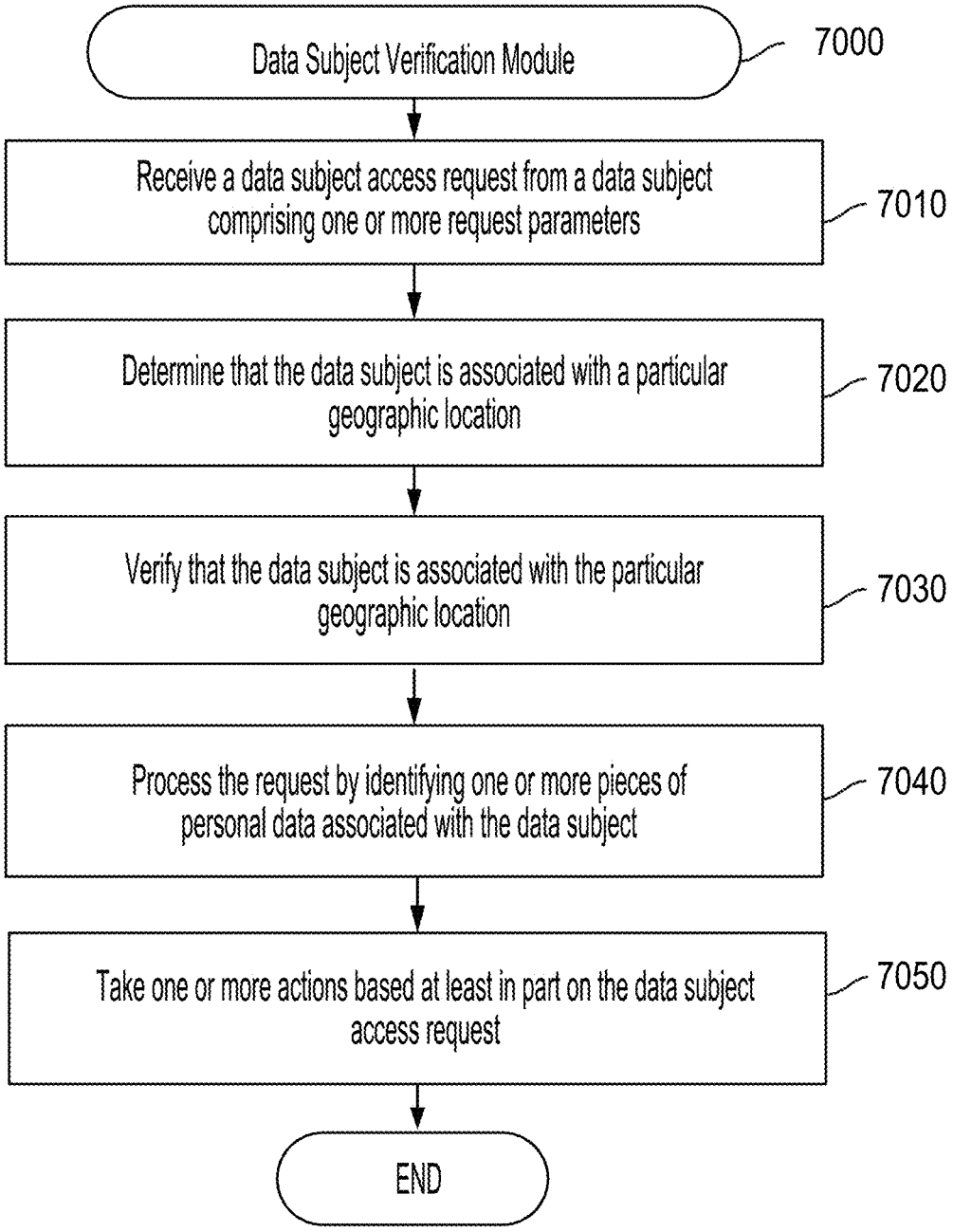

Data Subject Verification Module
7000
Receive a data subject access request from a data subject comprising one or more request parameters
7010
Determine that the data subject is associated with a particular geographic location
7020
Verify that the data subject is associated with the particular geographic location
7030
Process the request by identifying one or more pieces of personal data associated with the data subject
7040
Take one or more actions based at least in part on the data subject access request
7050
END

FIG. 70

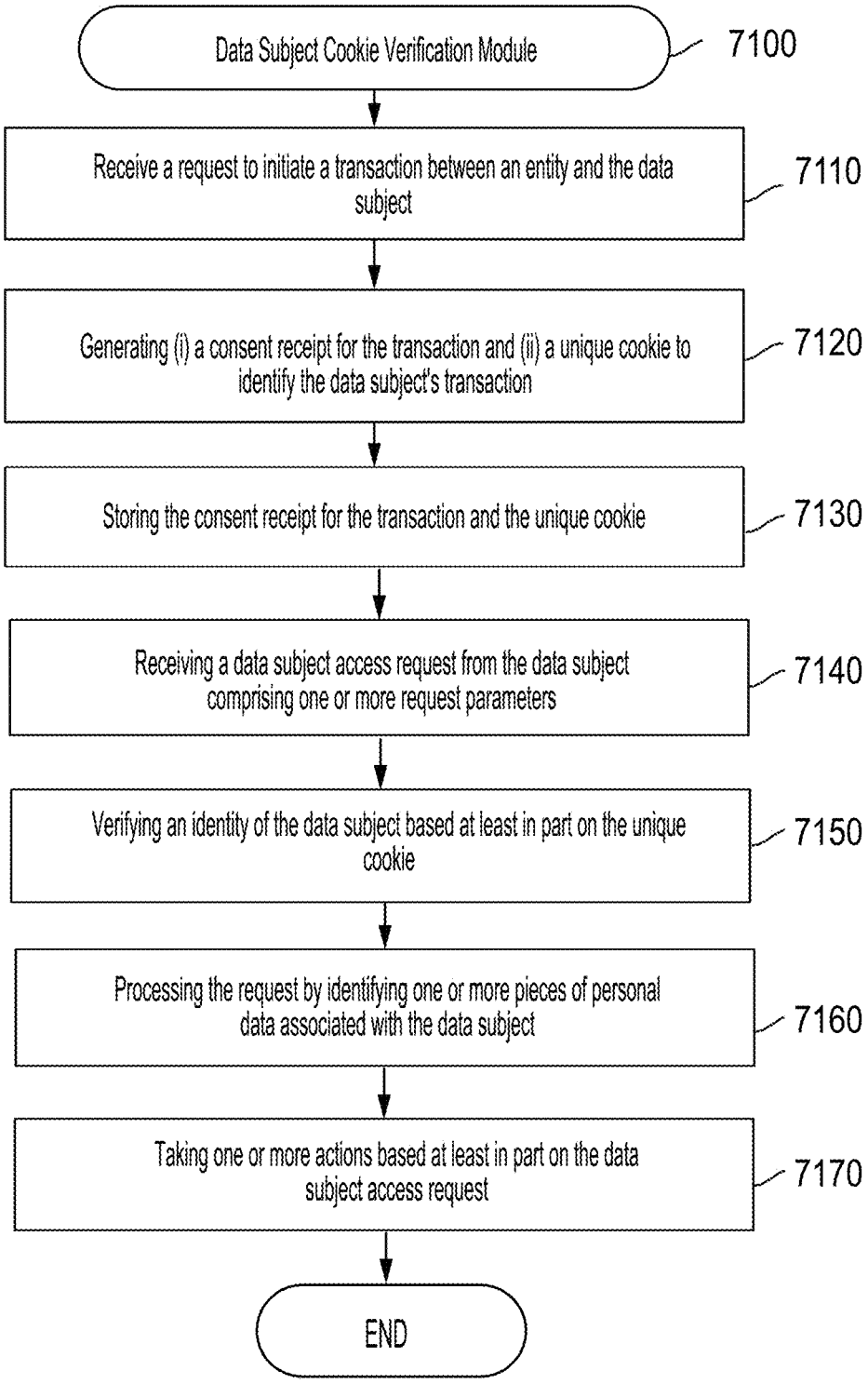

Data Subject Cookie Verification Module
7100
Receive a request to initiate a transaction between an entity and the data subject
7110
Generating (i) a consent receipt for the transaction and (ii) a unique cookie to identify the data subject's transaction
7120
Storing the consent receipt for the transaction and the unique cookie
7130
Receiving a data subject access request from the data subject comprising one or more request parameters
7140
Verifying an identity of the data subject based at least in part on the unique cookie
7150
Processing the request by identifying one or more pieces of personal data associated with the data subject
7160
Taking one or more actions based at least in part on the data subject access request
7170
END

FIG. 71

DATA SUBJECT ACCESS REQUEST PROCESSING SYSTEMS AND RELATED METHODS

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. patent application Ser. No. 17/475,241, filed Sep. 14, 2021, which is a continuation of U.S. patent application Ser. No. 17/135,445, filed Dec. 28, 2020, now U.S. Pat. No. 11,120,161, issued Sep. 14, 2021, which is a continuation of U.S. patent application Ser. No. 16/983,536, filed Aug. 3, 2020, now U.S. Pat. No. 10,878,127, issued Dec. 29, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 16/881,832, filed May 22, 2020, now U.S. Pat. No. 11,210,420, issued Dec. 28, 2021, which claims priority from U.S. Provisional Patent Application Ser. No. 62/852,832, filed May 24, 2019, and is also a continuation-in-part of U.S. patent application Ser. No. 16/834,812, filed Mar. 30, 2020, now U.S. Pat. No. 10,929,559, issued Feb. 23, 2021, which is a continuation of U.S. patent application Ser. No. 16/563,741, filed Sep. 6, 2019, now U.S. Pat. No. 10,607,028, issued Mar. 31, 2020, which claims priority from U.S. Provisional Patent Application Ser. No. 62/728,435, filed Sep. 7, 2018, and is also a continuation-in-part of U.S. patent application Ser. No. 16/410,566, filed May 13, 2019, now U.S. Pat. No. 10,452,866, issued Oct. 22, 2019, which is a continuation-in-part of U.S. patent application Ser. No. 16/055,083, filed Aug. 4, 2018, now U.S. Pat. No. 10,289,870, issued May 14, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/547,530, filed Aug. 18, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/996,208, filed Jun. 1, 2018, now U.S. Pat. No. 10,181,051, issued Jan. 15, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/537,839 filed Jul. 27, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/853,674, filed Dec. 22, 2017, now U.S. Pat. No. 10,019,597, issued Jul. 10, 2018, which claims priority from U.S. Provisional Patent Application Ser. No. 62/541,613, filed Aug. 4, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/619,455, filed Jun. 10, 2017, now U.S. Pat. No. 9,851,966, issued Dec. 26, 2017, which is a continuation-in-part of U.S. patent application Ser. No. 15/254,901, filed Sep. 1, 2016, now U.S. Pat. No. 9,729,583, issued Aug. 8, 2017, which claims priority from: (1) U.S. Provisional Patent Application Ser. No. 62/360,123, filed Jul. 8, 2016; (2) U.S. Provisional Patent Application Ser. No. 62/353,802, filed Jun. 23, 2016; and (3) U.S. Provisional Patent Application Ser. No. 62/348,695, filed Jun. 10, 2016. U.S. patent application Ser. No. 16/881,832 is also a continuation-in-part of U.S. patent application Ser. No. 16/552,765, filed Aug. 27, 2019, now U.S. Pat. No. 10,678,945, issued Jun. 9, 2020, which is a continuation-in-part of U.S. patent application Ser. No. 16/277,568, filed Feb. 15, 2019, now U.S. Pat. No. 10,440,062, issued Oct. 8, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/631,684, filed Feb. 17, 2018 and U.S. Provisional Patent Application Ser. No. 62/631,703, filed Feb. 17, 2018, and is also a continuation-in-part of U.S. patent application Ser. No. 16/159,634, filed Oct. 13, 2018, now U.S. Pat. No. 10,282,692, issued May 7, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/572,096, filed Oct. 13, 2017 and U.S. Provisional Patent Application Ser. No. 62/728,435, filed Sep. 7, 2018, and is also a continuation-in-part of U.S. patent application Ser. No. 16/055,083, filed Aug. 4, 2018, now U.S. Pat. No. 10,289,870, issued May 14, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/547,530, filed Aug. 18, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/996,208, filed Jun. 1, 2018, now U.S. Pat. No. 10,181,051, issued Jan. 15, 2019, which claims priority from U.S. Provisional Patent Application Ser. No. 62/537,839, filed Jul. 27, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/853,674, filed Dec. 22, 2017, now U.S. Pat. No. 10,019,597, issued Jul. 10, 2018, which claims priority from U.S. Provisional Patent Application Ser. No. 62/541,613, filed Aug. 4, 2017, and is also a continuation-in-part of U.S. patent application Ser. No. 15/619,455, filed Jun. 10, 2017, now U.S. Pat. No. 9,851,966, issued Dec. 26, 2017, which is a continuation-in-part of U.S. patent application Ser. No. 15/254,901, filed Sep. 1, 2016, now U.S. Pat. No. 9,729,583, issued Aug. 8, 2017, which claims priority from: (1) U.S. Provisional Patent Application Ser. No. 62/360,123, filed Jul. 8, 2016; (2) U.S. Provisional Patent Application Ser. No. 62/353,802, filed Jun. 23, 2016; and (3) U.S. Provisional Patent Application Ser. No. 62/348,695, filed Jun. 10, 2016. The disclosures of all of the above patent applications are hereby incorporated herein by reference in their entirety.

BACKGROUND

Over the past years, privacy and security policies, and related operations have become increasingly important. Breaches in security, leading to the unauthorized access of personal data (which may include sensitive personal data) have become more frequent among companies and other organizations of all sizes. Such personal data may include, but is not limited to, personally identifiable information (PII), which may be information that directly (or indirectly) identifies an individual or entity. Examples of PII include names, addresses, dates of birth, social security numbers, and biometric identifiers such as a person's fingerprints or picture. Other personal data may include, for example, customers' Internet browsing habits, purchase history, and even their preferences (e.g., likes and dislikes, as provided or obtained through social media).

To manage personal data, many companies have attempted to implement operational policies and processes that comply with certain rights related to the data subject's personal data that is collected, stored, or otherwise processed by an organization. These rights may include, for example, a right to obtain confirmation of whether a particular organization is processing their personal data, a right to obtain information about the purpose of the processing (e.g., one or more reasons for which the personal data was collected), and other such rights. Some regulations require organizations to comply with requests for such information (e.g., Data Subject Access Requests) within relatively short periods of time (e.g., 30 days). Accordingly, an organization's processing of such requests can require a significant amount of computing resources, especially when the organization is required to comply with such requests in a relatively short period of time. A significant challenge encountered by many organizations is that requests for personal data may originate from computing devices that are not authorized to make such requests (e.g., because the requests have not been directed by an individual entitled to the data responsive to the requests). For example, a data subject may submit a data processing request that includes particular requests to which the data subject is not entitled. Therefore, a need exists in the arts for improved systems and

methods for identifying and handling requests and confirming that a device or data subject submitting the request is entitled to make such a request prior to expending valuable computing resources on the processing of the request.

Existing systems for complying with such requests can be inadequate for producing and providing the required information within the required timelines. This is especially the case for large corporations, which may store data on several different platforms in differing locations. Accordingly, there is a need for improved systems and methods for complying with data subject access requests.

SUMMARY

In general, various aspects of the present disclosure provide methods, apparatuses, systems, computing devices, computing entities, and/or the like. In accordance with various aspects, a method is provided. Accordingly, the method comprises: (1) providing, by computing hardware, a query interface that is accessible via a public data network and that is configured for querying a plurality of data storage systems included in a private data network; (2) receiving, via the query interface and the public data network, a query comprising a data subject access request from a computing device; (3) accessing, by the computing hardware, a consent receipt key for a transaction associated with processing personal data for a data subject identified by the data subject access request; (4) accessing, by the computing hardware, transaction data for the transaction; (5) authenticating, by the computing hardware, the query by comparing the transaction data to the consent receipt key to determine that the transaction data comprises a subset of consent receipt key data associated with the consent receipt key; and (6) responsive to authenticating the query, facilitating, by the computing hardware, execution of processing operations or network communication for retrieving data responsive to the data subject access request from the plurality of data storage systems included in the private data network.

In various aspects, accessing the transaction data comprises accessing the transaction data on the computing device. In a particular aspect, the transaction data comprises a cookie. In some aspects, the transaction data identifies the consent receipt key. In some aspects, receiving the query comprises receiving the query via a web browser executing on the computing device, and accessing the transaction data comprises accessing the transaction data from a cookie store accessible to the web browser. In a particular aspect, the consent receipt key data comprises at least one of a transaction identifier for the transaction, a data subject identifier identifying the data subject, or an indication of consent provided by the data subject for the transaction, and the transaction data comprises at least one of the transaction identifier, the data subject identifier, and the consent receipt key. In some aspects, the method further comprises preventing, based on a failure to authenticate the query, execution of the processing operations or performing network communication for retrieving data responsive to the data subject access request from the plurality of data storage systems included in the private data network.

In accordance with various aspects, a system is provided comprising a non-transitory computer-readable medium storing instructions and a processing device communicatively coupled to the non-transitory computer-readable medium. The processing device is configured to execute the instructions and thereby perform operations similar to the steps recited above for the method. IN a particular embodiment, the operations comprise: (1) receiving, via a web browser on a user device, a data subject access request associated a data subject, the data subject access request comprising a data subject access request parameter; (2) accessing a consent receipt key for a transaction involving processing of personal data associated with the data subject as part of a transaction, the consent receipt key indicating consent, by the data subject, for the processing of personal data; (3) accessing transaction data for the transaction on the user device, the transaction data identifying the consent receipt key; (4) verifying an identity of the data subject based on receipt definitions associated with the consent receipt key and the transaction data; and (5) in response to verifying the identity of the data subject, processing the data subject access request based on the data subject access request parameter.

In some aspects, the transaction data comprises a unique cookie that is accessible to the web browser. In other aspects, the unique cookie and the consent receipt key were generated in response to initiation of the transaction. In a particular aspects, verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data comprises at least a subset of the receipt definitions. In such aspects, the receipt definitions may comprise at least one of a transaction identifier for the transaction, a data subject identifier identifying the data subject, or an indication of consent provided by the data subject for the transaction, and the transaction data may comprise at least one of the transaction identifier, the data subject identifier, and the consent receipt key. In one aspect, verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data and the receipt definitions identify the transaction. In some aspects, receiving the data subject access request via the web browser on the user device comprises receiving the data subject access request via a public data network, and processing the data subject access request based on the data subject access request parameter comprises initiating processing operations or network communication for retrieving the personal data from a plurality of storage locations in a private computing network

In addition, in accordance with various aspects, a non-transitory computer-readable medium having program code that is stored thereon. The program code executable by one or more processing devices performs operations similar to the steps recited above for the method. In some aspects, the operations comprise: (1) a data subject access request identifying a data subject, the data subject access request comprising a data subject access request parameter; (2) accessing a consent receipt key for a transaction involving processing of personal data associated with the data subject as part of a transaction, the consent receipt key indicating consent, by the data subject, for the processing of personal data; (3) accessing transaction data generated in response to initiation of the transaction; (4) verifying an identity of the data subject based on receipt definitions associated with the consent receipt key and the transaction data; and (5) in response to verifying the identity of the data subject, processing the data subject access request based on the data subject access request parameter. In some aspects, processing the data subject access request based on the data subject access request parameter comprises initiating processing operations or network communication for retrieving the personal data from a plurality of storage locations in a private computing network.

In particular aspects, the operations further preventing, based on a failure to verify the identity of the data subject, initiation of processing operations or network communica-

tion for retrieving data responsive to the data subject access request from the plurality of storage locations included in the private data network. In various aspects, receiving the data subject access request comprises receiving the data subject access request via a web browser executing on a computing device. In such aspects, accessing the transaction data may comprise accessing the transaction data from a cookie store accessible to the web browser. In a particular aspect, the cookie store is local to the computing device. In some aspects, verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data comprises at least a subset of the receipt definitions

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of a data subject access request fulfillment system are described below. In the course of this description, reference will be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. **1** depicts a data subject request processing and fulfillment system according to particular embodiments.

FIG. **2**A is a schematic diagram of a computer (such as the data model generation server **110**, or data model population server **120** of FIG. **1**) that is suitable for use in various embodiments of the data subject request processing and fulfillment system shown in FIG. **1**.

FIG. **2**B is a flow chart depicting exemplary steps executed by a Data Subject Access Request Routing Module according to a particular embodiment

FIGS. **3-43** are computer screen shots that demonstrate the operation of various embodiments.

FIGS. **44-49** depict various exemplary screen displays and user interfaces that a user of various embodiments of the system may encounter (FIGS. **47** and **48** collectively show four different views of a Data Subject Request Queue).

FIG. **50** is a flowchart showing an example of processes performed by an Orphaned Data Action Module **5000** according to various embodiments.

FIG. **51** is a flowchart showing an example of processes performed by a Personal Data Deletion and Testing Module **5100** according to various embodiments.

FIG. **52** is a flowchart showing an example of processes performed by a Data Risk Remediation Module **5200** according to various embodiments.

FIG. **53** is a flowchart showing an example of processes performed by a Central Consent Module **5300** according to various embodiments.

FIG. **54** is a flowchart showing an example of processes performed by a Data Transfer Risk Identification Module **5400** according to various embodiments.

FIG. **55** is a flowchart showing an example of steps performed by a Data Model Generation Module according to particular embodiments.

FIGS. **56-62** depict various exemplary visual representations of data models according to particular embodiments.

FIG. **63** is a flowchart showing an example of steps performed by a Data Model Population Module.

FIG. **64** is a flowchart showing an example of steps performed by a Data Population Questionnaire Generation Module.

FIG. **65** is a process flow for populating a data inventory according to a particular embodiment using one or more data mapping techniques.

FIG. **66** is a flowchart showing an example of steps performed by an Intelligent Identity Scanning Module.

FIG. **67** is schematic diagram of network architecture for an intelligent identity scanning system **2700** according to a particular embodiment.

FIG. **68** is a schematic diagram of an asset access methodology utilized by an intelligent identity scanning system **2700** in various embodiments of the system.

FIG. **69** is a flowchart showing an example of a processes performed by a Data Subject Access Request Fulfillment Module **2900** according to various embodiments.

FIG. **70** is a flow chart showing an example of a process performed by a Data Subject Verification Module according to particular embodiments.

FIG. **71** is a flow chart showing an example of a process performed by a Data Subject Cookie Verification Module according to particular embodiments.

DETAILED DESCRIPTION

Various embodiments now will be described more fully hereinafter with reference to the accompanying drawings. It should be understood that the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Overview

As previously noted, privacy and security policies, and related operations, have become increasingly important over the past years. As a result, many organizations have attempted to implement operational processes that comply with certain rights related to a data subject's personal data that is collected, stored, or otherwise processed by an organization. These rights may include, for example, a right to obtain confirmation of whether a particular organization is processing their personal data, a right to obtain information about the purpose of the processing (e.g., one or more reasons for which the personal data was collected), and other such rights. Some regulations require organizations to comply with requests for such information (e.g., Data Subject Access Requests) within relatively short periods of time (e.g., 30 days).

However, a technical challenge often encountered by many organizations in their processing of personal data while complying with a data subject's rights related to their personal data that is collected, stored, or otherwise processed by an organization is facilitating (e.g., allowing) the data subject's exercise of such rights when the personal data involved may exist over multiple data sources (e.g., computing devices, data storage, and/or the like) found within multiple data storage systems. As a result, an organization's processing of requests received from data subjects (e.g., individuals) who are exercising their rights related to their personal data can require a significant amount of computing resources.

For instance, many organizations provide a publicly accessible query interface through which data subjects (or lawful representatives thereof) can submit requests (e.g., data subject access requests) related to their personal data being processed by the organizations. For example, many organizations provide a website that is accessible by data subjects over a public data network such as the Internet. Here, the website may include a web form that can be used by the data subjects to submit requests related to the data subjects' personal data being processed by the organizations. Therefore, a data subject wishing to exercise their

rights can simply visit an organization's website and use the webform to submit a query that includes a request related to a personal data right that is then often required to be fulfilled by the organization in a timely manner. Since the query interface (e.g., website) is often publicly available, an organization can receive a considerable number of requests at any given time that then requires the organization to devote a significant number of computing resources to timely fulfill the requests. This can become even more of a substantial challenge as personal data collected, stored, or otherwise processed by an organization increases in volume and/or is collected, stored, or otherwise processed over an increasing number of data sources involving multiple data storage systems that are in communication over one or more private data networks.

Another technical challenge encountered by many organizations is the receiving and processing of requests by data subjects, who may, for example, not be entitled to the requested processing of data. Such requests can prove to be a technical challenge for many organizations in that the organizations can be subject to a wasteful devotion of computing resources in processing such requests when the resources could be used for more meaningful, valid, and/or legitimate purposes. As such, it may be beneficial for an organization to authenticate a request prior to initiating processing operations and/or network communication for retrieving data responsive to a request. Authenticating the request may include, for example, confirming an identity of a user submitting a request, authenticating a computing device as a valid computing device for submitting such a request on behalf of an individual, etc. Therefore, many organizations are faced with the challenge of a request prior to processing, to eliminate and/or limit the processing of such requests to avoid wasteful use of computing resources.

Accordingly, various embodiments of the present disclosure overcome many of the technical challenges mentioned above by authenticating a request or query prior to executing processing operations or network communication for retrieving data responsive to the request by comparing transaction data (e.g., for a transaction under which an individual had provided consent for the processing of their sensitive data) to consent receipt key data generated in response to an initiation of the transaction. As described in further detail herein, the present disclosure may access a consent receipt key for a transaction associated with processing personal data for a data subject identified by a particular request, and then compare consent receipt key data to the transaction data do determine whether the transaction data comprises a subset of the consent receipt key data. For example, when initiating a transaction (e.g., that involves processing personal data of a data subject), a computing system may generate a consent receipt key indicating, for example, an identifier for the transaction, an identifier for the data subject that provided the consent, etc.). A computing system may further generate transaction data (e.g., for storage on a computing device from which the transaction was initiated by the data subject). Various embodiments of the present disclosure may then enable a comparison of the consent receipt key data to the transaction data stored on the computing device in order to authenticate the device as a device that is authorized to submit data subject access requests related to sensitive data collected and/or processed under the transaction. In various aspects, the transaction data may be stored as a cookie accessible to the computing device.

A data model generation and population system, according to particular embodiments, is configured to generate a data model (e.g., one or more data models) that maps one or more relationships between and/or among a plurality of data assets utilized by a corporation or other entity (e.g., individual, organization, etc.) in the context, for example, of one or more business processes. In particular embodiments, each of the plurality of data assets (e.g., data systems) may include, for example, any entity that collects, processes, contains, and/or transfers data (e.g., such as a software application, "internet of things" computerized device, database, web site, data-center, server, etc.). For example, a first data asset may include any software or device (e.g., server or servers) utilized by a particular entity for such data collection, processing, transfer, storage, etc.

As shown in FIGS. **4** and **5**, in various embodiments, the data model may store the following information: (1) the organization that owns and/or uses a particular data asset (a primary data asset, which is shown in the center of the data model in FIG. **4**); (2) one or more departments within the organization that are responsible for the data asset; (3) one or more software applications that collect data (e.g., personal data) for storage in and/or use by the data asset (e.g., or one or more other suitable collection assets from which the personal data that is collected, processed, stored, etc. by the primary data asset is sourced); (4) one or more particular data subjects (or categories of data subjects) that information is collected from for use by the data asset; (5) one or more particular types of data that are collected by each of the particular applications for storage in and/or use by the data asset; (6) one or more individuals (e.g., particular individuals or types of individuals) that are permitted to access and/or use the data stored in, or used by, the data asset; (7) which particular types of data each of those individuals are allowed to access and use; and (8) one or more data assets (destination assets) that the data is transferred to for other use, and which particular data is transferred to each of those data assets. As shown in FIGS. **6** and **7**, the system may also optionally store information regarding, for example, which business processes and processing activities utilize the data asset.

In particular embodiments, the data model stores this information for each of a plurality of different data assets and may include links between, for example, a portion of the model that provides information for a first particular data asset and a second portion of the model that provides information for a second particular data asset.

In various embodiments, the data model generation and population system may be implemented in the context of any suitable privacy management system that is configured to ensure compliance with one or more legal or industry standards related to the collection and/or storage of private information. In various embodiments, a particular organization, sub-group, or other entity may initiate a privacy campaign or other activity (e.g., processing activity) as part of its business activities. In such embodiments, the privacy campaign may include any undertaking by a particular organization (e.g., such as a project or other activity) that includes the collection, entry, and/or storage (e.g., in memory) of any personal data associated with one or more individuals. In particular embodiments, a privacy campaign may include any project undertaken by an organization that includes the use of personal data, or any other activity that could have an impact on the privacy of one or more individuals.

In any embodiment described herein, personal data may include, for example: (1) the name of a particular data subject (which may be a particular individual); (2) the data subject's address; (3) the data subject's telephone number;

(4) the data subject's e-mail address; (5) the data subject's social security number; (6) information associated with one or more of the data subject's credit accounts (e.g., credit card numbers); (7) banking information for the data subject; (8) location data for the data subject (e.g., their present or past location); (9) internet search history for the data subject; and/or (10) any other suitable personal information, such as other personal information discussed herein. In particular embodiments, such personal data may include one or more cookies (e.g., where the individual is directly identifiable or may be identifiable based at least in part on information stored in the one or more cookies).

In particular embodiments, when generating a data model, the system may, for example: (1) identify one or more data assets associated with a particular organization; (2) generate a data inventory for each of the one or more data assets, where the data inventory comprises information such as: (a) one or more processing activities associated with each of the one or more data assets, (b) transfer data associated with each of the one or more data assets (data regarding which data is transferred to/from each of the data assets, and which data assets, or individuals, the data is received from and/or transferred to, (c) personal data associated with each of the one or more data assets (e.g., particular types of data collected, stored, processed, etc. by the one or more data assets), and/or (d) any other suitable information; and (3) populate the data model using one or more suitable techniques.

In particular embodiments, the one or more techniques for populating the data model may include, for example: (1) obtaining information for the data model by using one or more questionnaires associated with a particular privacy campaign, processing activity, etc.; (2) using one or more intelligent identity scanning techniques discussed herein to identify personal data stored by the system and map such data to a suitable data model, data asset within a data model, etc.; (3) obtaining information for the data model from a third-party application (or other application) using one or more application programming interfaces (API); and/or (4) using any other suitable technique.

In particular embodiments, the system is configured to generate and populate a data model substantially on the fly (e.g., as the system receives new data associated with particular processing activities). In still other embodiments, the system is configured to generate and populate a data model based at least in part on existing information stored by the system (e.g., in one or more data assets), for example, using one or more suitable scanning techniques described herein.

As may be understood in light of this disclosure, a particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, a particular organization may store personal data in a plurality of different locations which may include one or more known and/or unknown locations. By generating and populating a data model of one or more data assets that are involved in the collection, storage and processing of such personal data, the system may be configured to create a data model that facilitates a straightforward retrieval of information stored by the organization as desired. For example, in various embodiments, the system may be configured to use a data model in substantially automatically responding to one or more data access requests by an individual (e.g., or other organization). Various embodiments of a system for generating and populating a data model are described more fully below.

Ticket management systems, according to various embodiments, are adapted to receive data subject access requests (DSAR's) from particular data subjects, and to facilitate the timely processing of valid DSAR's by an appropriate respondent. In particular embodiments, the ticket management system receives DSAR's via one or more webforms that each may, for example, respectively be accessed via an appropriate link/button on a respective web page. In other embodiments, the system may receive DSAR's through any other suitable mechanism, such as via a computer software application (e.g., a messaging application such as Slack, Twitter), via a chat bot, via generic API input from another system, or through entry by a representative who may receive the information, for example, via suitable paper forms or over the phone.

The ticket management system may include a webform creation tool that is adapted to allow a user to create customized webforms for receiving DSAR's from various different data subject types and for routing the requests to appropriate individuals for processing. The webform creation tool may, for example, allow the user to specify the language that the form will be displayed in, what particular information is to be requested from the data subject and/or provided by the data subject, who any DSAR's that are received via the webform will be routed to, etc. In particular embodiments, after the user completes their design of the webform, the webform creation tool generates code for the webform that may be cut and then pasted into a particular web page.

The system may be further adapted to facilitate processing of DSAR's that are received via the webforms, or any other suitable mechanism. For example, the ticket management system may be adapted to execute one or more of the following steps for each particular DSAR received via the webforms (or other suitable mechanism) described above: (1) before processing the DSAR, confirm that the DSAR was actually submitted by the particular data subject of the DSAR (or, for example, by an individual authorized to make the DSAR on the data subject's behalf, such as a parent, guardian, power-of-attorney holder, etc.)—any suitable method may be used to confirm the identity of the entity/individual submitting the DSAR—for example, if the system receives the DSAR via a third-party computer system, the system may validate authentication via API secret, or by requiring a copy of one or more particular legal documents (e.g., a particular contract between two particular entities)—the system may validate the identity of an individual by, for example, requiring the individual (e.g., data subject) to provide particular account credentials, by requiring the individual to provide particular out-of-wallet information, through biometric scanning of the individual (e.g., finger or retinal scan), or via any other suitable identity verification technique; (2) if the DSAR was not submitted by the particular data subject, deny the request; (3) if the DSAR was submitted by the particular data subject, advance the processing of the DSAR; (4) route the DSAR to the correct individual(s) or groups internally for handling; (5) facilitate the assignment of the DSAR to one or more other individuals for handling of one or more portions of the DSAR; (6) facilitate the suspension of processing of the data subject's data by the organization; and/or (7) change the policy

according to which the data subject's personal data is retained and/or processed by the system. In particular embodiments, the system may perform any one or more of the above steps automatically. The system then generates a receipt for the DSAR request that the user can use as a transactional record of their submitted request.

In particular embodiments, the ticket management system may be adapted to generate a graphical user interface (e.g., a DSAR request-processing dashboard) that is adapted to allow a user (e.g., a privacy officer of an organization that is receiving the DSAR) to monitor the progress of any of the DSAR requests. The GUI interface may display, for each DSAR, for example, an indication of how much time is left (e.g., quantified in days and/or hours) before a legal and/or internal deadline to fulfill the request. The system may also display, for each DSAR, a respective user-selectable indicium that, when selected, may facilitate one or more of the following: (1) verification of the request; (2) assignment of the request to another individual; (3) requesting an extension to fulfill the request; (4) rejection of the request; or (5) suspension of the request.

As noted immediately above, and elsewhere in this application, in particular embodiments, any one or more of the above steps may be executed by the system automatically. As a particular example, the system may be adapted to automatically verify the identity of the DSAR requestor and then automatically fulfill the DSAR request by, for example, obtaining the requested information via a suitable data model and communicating the information to the requestor. As another particular example, the system may be configured to automatically route the DSAR to the correct individual for handling based at least in part on one or more pieces of information provided (e.g., in the webform).

In various embodiments, the system may be adapted to prioritize the processing of DSAR's based on metadata about the data subject of the DSAR. For example, the system may be adapted for: (1) in response to receiving a DSAR, obtaining metadata regarding the data subject; (2) using the metadata to determine whether a priority of the DSAR should be adjusted based on the obtained metadata; and (3) in response to determining that the priority of the DSAR should be adjusted based on the obtained metadata, adjusting the priority of the DSAR.

Examples of metadata that may be used to determine whether to adjust the priority of a particular DSAR include: (1) the type of request; (2) the location from which the request is being made; (3) the country of residency of the data subject and, for example, that county's tolerance for enforcing DSAR violations; (4) current sensitivities to world events; (5) a status of the requestor (e.g., especially loyal customer); or (6) any other suitable metadata.

In particular embodiments, any entity (e.g., organization, company, etc.) that collects, stores, processes, etc. personal data may require one or more of: (1) consent from a data subject from whom the personal data is collected and/or processed; and/or (2) a lawful basis for the collection and/or processing of the personal data. In various embodiments, the entity may be required to, for example, demonstrate that a data subject has freely given specific, informed, and unambiguous indication of the data subject's agreement to the processing of his or her personal data for one or more specific purposes (e.g., in the form of a statement or clear affirmative action). As such, in particular embodiments, an organization may be required to demonstrate a lawful basis for each piece of personal data that the organization has collected, processed, and/or stored. In particular, each piece of personal data that an organization or entity has a lawful basis to collect and process may be tied to a particular processing activity undertaken by the organization or entity.

A particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, because of the number of processing activities that an organization may undertake, and the amount of data collected as part of those processing activities over time, one or more data systems associated with an entity or organization may store or continue to store data that is not associated with any particular processing activity (e.g., any particular current processing activity). Under various legal and industry standards related to the collection and storage of personal data, the organization or entity may not have or may no longer have a legal basis to continue to store the data. As such, organizations and entities may require improved systems and methods to identify such orphaned data, and take corrective action, if necessary (e.g., to ensure that the organization may not be in violation of one or more legal or industry regulations).

In various embodiments, an orphaned personal data identification system may be configured to generate a data model (e.g., one or more data models) that maps one or more relationships between and/or among a plurality of data assets utilized by a corporation or other entity (e.g., individual, organization, etc.) in the context, for example, of one or more business processes or processing activities. In particular embodiments, the system is configured to generate and populate a data model substantially on the fly (e.g., as the system receives new data associated with particular processing activities). In still other embodiments, the system is configured to generate and populate a data model based at least in part on existing information stored by the system (e.g., in one or more data assets), for example, using one or more suitable scanning techniques. In still other embodiments, the system is configured to access an existing data model that maps personal data stored by one or more organization systems to particular associated processing activities.

In various embodiments, the system may analyze the data model to identify personal data that has been collected and stored using one or more computer systems operated and/or utilized by a particular organization where the personal data is not currently being used as part of any privacy campaigns, processing activities, etc. undertaken by the particular organization. This data may be described as orphaned data. In some circumstances, the particular organization may be exposed to an increased risk that the data may be accessed by a third party (e.g., cybercrime) or that the particular organization may not be in compliance with one or more legal or industry requirements related to the collection, storage, and/or processing of this orphaned data.

Additionally, in some implementations, in response to the termination of a particular privacy campaign, processing activity, (e.g., manually or automatically), the system may be configured to analyze the data model to determine whether any of the personal data that has been collected and stored by the particular organization is now orphaned data (e.g., whether any personal data collected and stored as part

of the now-terminated privacy campaign is being utilized by any other processing activity, has some other legal basis for its continued storage, etc.).

In additional implementations in response to determining that a particular privacy campaign, processing activity, etc. has not been utilized for a period of time (e.g., a day, month, year), the system may be configured to terminate the particular privacy campaign, processing activity, etc. or prompt one or more individuals associated with the particular organization to indicate whether the particular privacy campaign, processing activity, etc. should be terminated or otherwise discontinued.

For example, a particular processing activity may include transmission of a periodic advertising e-mail for a particular company (e.g., a hardware store). As part of the processing activity, the particular company may have collected and stored e-mail addresses for customers that elected to receive (e.g., consented to the receipt of) promotional e-mails. In response to determining that the particular company has not sent out any promotional e-mails for at least a particular amount of time (e.g., for at least a particular number of months), the system may be configured to: (1) automatically terminate the processing activity; (2) identify any of the personal data collected as part of the processing activity that is now orphaned data (e.g., the e-mail addresses); and (3) automatically delete the identified orphaned data. The processing activity may have ended for any suitable reason (e.g., because the promotion that drove the periodic e-mails has ended). As may be understood in light of this disclosure, because the particular organization no longer has a valid basis for continuing to store the e-mail addresses of the customers once the e-mail addresses are no longer being used to send promotional e-mails, the organization may wish to substantially automate the removal of personal data stored in its computer systems that may place the organization in violation of one or more personal data storage rules or regulations.

When the particular privacy campaign, processing activity, etc. is terminated or otherwise discontinued, the system may use the data model to determine if any of the associated personal data that has been collected and stored by the particular organization is now orphaned data.

In various embodiments, the system may be configured to identify orphaned data of a particular organization and automatically delete the data. In some implementations, in response to identifying the orphaned data, the system may present the data to one or more individuals associated with the particular organization (e.g., a privacy officer) and prompt the one or more individuals to indicate why the orphaned data is being stored by the particular organization. The system may then enable the individual to provide one or more valid reasons for the data's continued storage, or enable the one or more individuals to delete the particular orphaned data. In some embodiments, the system may automatically delete the orphaned data if, for example: (1) in response to determining that a reason provided by the individual is not a sufficient basis for the continued storage of the personal data; (2) the individual does not respond to the request to provide one or more valid reasons in a timely manner; (3) etc. In some embodiments, one or more other individuals may review the response provided indicating why the orphaned data is being stored, and in some embodiments, the one or more other individuals can delete the particular orphaned data.

In various embodiments, the system may be configured to review the data collection policy (e.g., how data is acquired, security of data storage, who can access the data, etc.) for the particular organization as well as one or more data retention metrics for the organization. For example, the one or more data retention metrics may include how much personal data is being collected, how long the data is held, how many privacy campaigns or other processes are using the personal data, etc. Additionally, the system may compare the particular organization's data collection policy and data retention metrics to the industry standards (e.g., in a particular field, based on a company size, etc.). In various embodiments, the system may be configured to generate a report that includes the comparison and provide the report to the particular organization (e.g., in electronic format).

In particular embodiments, the system may be configured advise the particular organization to delete data and identify particular data that should be deleted. In some embodiments, the system may automatically delete particular data (e.g., orphaned data). Further, the system may be configured to calculate and provide a risk score for particular data or the organization's data collection policy overall. In particular embodiments, the system may be configured to calculate the risk score based on the combinations of personal data elements in the data inventory of the organization (e.g., where an individual's phone number is stored in one location and their mailing address is stored in another location), and as such the risk may be increased because the additional pieces of personal information can make the stored data more sensitive.

In particular embodiments, any entity (e.g., organization, company, etc.) that collects, stores, processes, etc. personal data may require one or more of: (1) consent from a data subject from whom the personal data is collected and/or processed; and/or (2) a lawful basis for the collection and/or processing of the personal data. In various embodiments, the entity may be required to, for example, demonstrate that a data subject has freely given specific, informed, and unambiguous indication of the data subject's agreement to the processing of his or her personal data for one or more specific purposes (e.g., in the form of a statement or clear affirmative action). As such, in particular embodiments, an organization may be required to demonstrate a lawful basis for each piece of personal data that the organization has collected, processed, and/or stored. In particular, each piece of personal data that an organization or entity has a lawful basis to collect and process may be tied to a particular processing activity undertaken by the organization or entity.

A particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, because of the number of processing activities that an organization may undertake, and the amount of data collected as part of those processing activities over time, one or more data systems associated with an entity or organization may store or continue to store data that is not associated with any particular processing activity (e.g., any particular current processing activity). Under various legal and industry standards related to the collection and storage of personal data, such data may not have or may no longer have a legal basis for the organization or entity to continue to store the data. As such, organizations and entities may require improved systems and methods to maintain an inventory of

data assets utilized to process and/or store personal data for which a data subject has provided consent for such storage and/or processing.

In various embodiments, the system is configured to provide a third-party data repository system to facilitate the receipt and centralized storage of personal data for each of a plurality of respective data subjects, as described herein. Additionally, the third-party data repository system is configured to interface with a centralized consent receipt management system.

In particular embodiments, the system may be configured to use one or more website scanning tools to, for example, identify a form (e.g., a webform) and locate a data asset where the input data is transmitted (e.g., Salesforce). Additionally, the system may be configured to add the data asset to the third-party data repository (e.g., and/or data map/data inventory) with a link to the form. In response to a user inputting form data (e.g., name, address, credit card information, etc.) of the form and submitting the form, the system may, based on the link to the form, create a unique subject identifier to submit to the third-party data repository and, along with the form data, to the data asset. Further, the system may use the unique subject identifier of a user to access and update each of the data assets of the particular organization. For example, in response to a user submitting a data subject access request to delete the user's personal data that the particular organization has stored, the system may use the unique subject identifier of the user to access and delete the user's personal data stored in all of the data assets (e.g., Salesforce, Eloqua, Marketo, etc.) utilized by the particular organization.

The system may, for example: (1) generate, for each of a plurality of data subjects, a respective unique subject identifier in response to submission, by each data subject, of a particular form; (2) maintain a database of each respective unique subject identifier; and (3) electronically link each respective unique subject identifier to each of: (A) a form initially submitted by the user; and (B) one or more data assets that utilize data received from the data subject via the form.

In various embodiments, the system may be configured to, for example: (1) identify a form used to collect one or more pieces of personal data, (2) determine a data asset of a plurality of data assets of the organization where input data of the form is transmitted, (3) add the data asset to the third-party data repository with an electronic link to the form, (4) in response to a user submitting the form, create a unique subject identifier to submit to the third-party data repository and, along with the form data provided by the user in the form, to the data asset, (5) submit the unique subject identifier and the form data provided by the user in the form to the third-party data repository and the data asset, and (6) digitally store the unique subject identifier and the form data provided by the user in the form in the third-party data repository and the data asset.

In some embodiments, the system may be further configured to, for example: (1) receive a data subject access request from the user (e.g., a data subject rights' request, a data subject deletion request, etc.), (2) access the third-party data repository to identify the unique subject identifier of the user, (3) determine which data assets of the plurality of data assets of the organization include the unique subject identifier, (4) access personal data of the user stored in each of the data assets of the plurality of data assets of the organization that include the unique subject identifier, and (5) take one or more actions based on the data subject access request (e.g., delete the accessed personal data in response to a data subject deletion request).

Various privacy and security policies (e.g., such as the European Union's General Data Protection Regulation, and other such policies) may provide data subjects (e.g., individuals, organizations, or other entities) with certain rights related to the data subject's personal data that is collected, stored, or otherwise processed by an entity. In particular, under various privacy and security policies, a data subject may be entitled to a right to erasure of any personal data associated with that data subject that has been at least temporarily stored by the entity (e.g., a right to be forgotten). In various embodiments, under the right to erasure, an entity (e.g., a data controller on behalf of another organization) may be obligated to erase personal data without undue delay under one or more of the following conditions: (1) the personal data is no longer necessary in relation to a purpose for which the data was originally collected or otherwise processed; (2) the data subject has withdrawn consent on which the processing of the personal data is based (e.g., and there is no other legal grounds for such processing); (3) the personal data has been unlawfully processed; (4) the data subject has objected to the processing and there is no overriding legitimate grounds for the processing of the data by the entity; and/or (5) for any other suitable reason or under any other suitable conditions.

In particular embodiments, a personal data deletion system may be configured to: (1) at least partially automatically identify and delete personal data that an entity is required to erase under one or more of the conditions discussed above; and (2) perform one or more data tests after the deletion to confirm that the system has, in fact, deleted any personal data associated with the data subject.

In particular embodiments, in response to a data subject submitting a request to delete their personal data from an entity's systems, the system may, for example: (1) automatically determine where the data subject's personal data is stored; and (2) in response to determining the location of the data (which may be on multiple computing systems), automatically facilitate the deletion of the data subject's personal data from the various systems (e.g., by automatically assigning a plurality of tasks to delete data across multiple business systems to effectively delete the data subject's personal data from the systems). In particular embodiments, the step of facilitating the deletion may comprise, for example: (1) overwriting the data in memory; (2) marking the data for overwrite; (2) marking the data as free (e.g., deleting a directory entry associated with the data); and/or (3) using any other suitable technique for deleting the personal data. In particular embodiments, as part of this process, the system may use any suitable data modelling technique to efficiently determine where all of the data subject's personal data is stored.

In various embodiments, the system may be configured to store (e.g., in memory) an indication that the data subject has requested to delete any of their personal data stored by the entity has been processed. Under various legal and industry policies/standards, the entity may have a certain period of time (e.g., a number of days) in order to comply with the one or more requirements related to the deletion or removal of personal data in response to receiving a request from the data subject or in response to identifying one or more of the conditions requiring deletion discussed above. In response to the receiving of an indication that the deletion request for the data subject's personal data has been processed or the certain period of time (described above) has passed, the

system may be configured to perform a data test to confirm the deletion of the data subject's personal data.

In particular embodiments, when performing the data test, the system may be configured to provide an interaction request to the entity on behalf of the data subject. In particular embodiments, the interaction request may include, for example, a request for one or more pieces of data associated with the data subject (e.g., account information, etc.). In various embodiments, the interaction request is a request to contact the data subject (e.g., for any suitable reason). The system may, for example, be configured to substantially automatically complete a contact-request form (e.g., a webform made available by the entity) on behalf of the data subject. In various embodiments, when automatically completing the form on behalf of the data subject, the system may be configured to only provide identifying data, but not provide any contact data. In response to submitting the interaction request (e.g., submitting the webform), the system may be configured to determine whether the one or more computers systems have generated and/or transmitted a response to the data subject. The system may be configured to determine whether the one or more computers systems have generated and/or transmitted the response to the data subject by, for example, analyzing one or more computer systems associated with the entity to determine whether the one or more computer systems have generated a communication to the data subject (e.g., automatically) for transmission to an e-mail address or other contact method associated with the data subject, generated an action-item for an individual to contact the data subject at a particular contact number, etc.

In response to determining that the one or more computer systems has generated and/or transmitted the response to the data subject, the system may be configured to determine that the one or more computer systems has not complied with the data subject's request for deletion of their personal data from the one or more computers systems associated with the entity. In response, the system may generate an indication that the one or more computer systems has not complied with the data subject's request for deletion of their personal data from the one or more computers systems have, and store the indication in computer memory.

To perform the data test, for example, the system may be configured to: (1) access (e.g., manually or automatically) a form for the entity (e.g., a web-based "Contact Us" form); (2) input a unique identifier associated with the data subject (e.g., a full name or customer ID number) without providing contact information for the data subject (e.g., mailing address, phone number, email address, etc.); and (3) input a request, within the form, for the entity to contact the data subject to provide information associated with the data subject (e.g., the data subject's account balance with the entity). In response to submitting the form to the entity, the system may be configured to determine whether the data subject is contacted (e.g., via a phone call or email) by the one or more computer systems (e.g., automatically). In response to determining that the data subject has been contacted following submission of the form, the system may determine that the one or more computer systems have not fully deleted the data subject's personal data (e.g., because the one or more computer systems must still be storing contact information for the data subject in at least one location).

In particular embodiments, the system is configured to generate one or more test profiles for one or more test data subjects. For each of the one or more test data subjects, the system may be configured to generate and store test profile data such as, for example: (1) name; (2) address; (3) telephone number; (4) e-mail address; (5) social security number; (6) information associated with one or more credit accounts (e.g., credit card numbers); (7) banking information; (8) location data; (9) internet search history; (10) non-credit account data; and/or (11) any other suitable test data. The system may then be configured to at least initially consent to processing or collection of personal data for the one or more test data subjects by the entity. The system may then request deletion, by the entity, of any personal data associated with a particular test data subject. In response to requesting the deletion of data for the particular test data subject, the system may then take one or more actions using the test profile data associated with the particular test data subjects in order to confirm that the one or more computers systems have, in fact, deleted the test data subject's personal data (e.g., any suitable action described herein). The system may, for example, be configured to: (1) initiate a contact request on behalf of the test data subject; (2) attempt to login to one or more user accounts that the system had created for the particular test data subject; and/or (3) take any other action, the effect of which could indicate a lack of complete deletion of the test data subject's personal data.

In response to determining that the one or more computer systems have not fully deleted a data subject's (or test data subject's) personal data, the system may then be configured, in particular embodiments, to: (1) flag the data subject's personal data for follow up by one or more privacy officers to investigate the lack of deletion; (2) perform one or more scans of one or more computing systems associated with the entity to identify any residual personal data that may be associated with the data subject; (3) generate a report indicating the lack of complete deletion; and/or (4) take any other suitable action to flag for follow-up the data subject, personal data, initial request to be forgotten, etc.

The system may, for example, be configured to test to ensure the data has been deleted by: (1) submitting a unique token of data through a form to a system (e.g., mark to); (2) in response to passage of an expected data retention time, test the system by calling into the system after the passage of the data retention time to search for the unique token. In response to finding the unique token, the system may be configured to determine that the data has not been properly deleted.

In various embodiments, a system may be configured to substantially automatically determine whether to take one or more actions in response to one or more identified risk triggers. For example, an identified risk trigger may be that a data asset for an organization is hosted in only one particular location thereby increasing the scope of risk if the location were infiltrated (e.g., via cybercrime). In particular embodiments, the system is configured to substantially automatically perform one or more steps related to the analysis of and response to the one or more potential risk triggers discussed above. For example, the system may substantially automatically determine a relevance of a risk posed by (e.g., a risk level) the one or more potential risk triggers based at least in part on one or more previously-determined responses to similar risk triggers. This may include, for example, one or more previously determined responses for the particular entity that has identified the current risk trigger, one or more similarly situated entities, or any other suitable entity or potential trigger.

In particular embodiments, the system may, for example, be configured to: (1) receive risk remediation data for a plurality of identified risk triggers from a plurality of different entities; (2) analyze the risk remediation data to

determine a pattern in assigned risk levels and determined response to particular risk triggers; and (3) develop a model based on the risk remediation data for use in facilitating an automatic assessment of and/or response to future identified risk triggers.

In some embodiments, when a change or update is made to one or more processing activities and/or data assets (e.g., a database associated with a particular organization), the system may use data modeling techniques to update the risk remediation data for use in facilitating an automatic assessment of and/or response to future identified risk triggers. In various embodiments, when a privacy campaign, processing activity, etc. of the particular organization is modified (e.g., add, remove, or update particular information), then the system may use the risk remediation data for use in facilitating an automatic assessment of and/or response to future identified risk triggers.

In particular embodiments, the system may, for example, be configured to: (1) access risk remediation data for an entity that identifies one or more suitable actions to remediate a risk in response to identifying one or more data assets of the entity that may be affected by one or more potential risk triggers; (2) receive an indication of an update to the one or more data assets; (3) identify one or more potential updated risk triggers for an entity; (4) assess and analyze the one or more potential updated risk triggers to determine a relevance of a risk posed to the entity by the one or more potential updated risk triggers; (5) use one or more data modeling techniques to identify one or more data assets associated with the entity that may be affected by the risk; and (6) update the risk remediation data to include the one or more actions to remediate the risk in response to identifying the one or more potential updated risk triggers.

In any embodiment described herein, an automated classification system may be configured to substantially automatically classify one or more pieces of personal information in one or more documents (e.g., one or more text-based documents, one or more spreadsheets, one or more PDFs, one or more webpages, etc.). In particular embodiments, the system may be implemented in the context of any suitable privacy compliance system, which may, for example, be configured to calculate and assign a sensitivity score to a particular document based at least in part on one or more determined categories of personal information (e.g., personal data) identified in the one or more documents. As understood in the art, the storage of particular types of personal information may be governed by one or more government or industry regulations. As such, it may be desirable to implement one or more automated measures to automatically classify personal information from stored documents (e.g., to determine whether such documents may require particular security measures, storage techniques, handling, whether the documents should be destroyed, etc.).

Exemplary Technical Platforms

As will be appreciated by one skilled in the relevant field, the present invention may be, for example, embodied as a computer system, a method, or a computer program product. Accordingly, various embodiments may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, particular embodiments may take the form of a computer program product stored on a computer-readable storage medium having computer-readable instructions (e.g., software) embodied in the storage medium. Various embodiments may take the form of web-implemented computer software. Any suitable computer-readable storage medium may be utilized including, for example, hard disks, compact disks, DVDs, optical storage devices, and/or magnetic storage devices.

Various embodiments are described below with reference to block diagrams and flowchart illustrations of methods, apparatuses (e.g., systems), and computer program products. It should be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by a computer executing computer program instructions. These computer program instructions may be loaded onto a general-purpose computer, special-purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus to create means for implementing the functions specified in the flowchart block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner such that the instructions stored in the computer-readable memory produce an article of manufacture that is configured for implementing the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions that execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

Accordingly, blocks of the block diagrams and flowchart illustrations support combinations of mechanisms for performing the specified functions, combinations of steps for performing the specified functions, and program instructions for performing the specified functions. It should also be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, can be implemented by special purpose hardware-based computer systems that perform the specified functions or steps, or combinations of special purpose hardware and other hardware executing appropriate computer instructions.

Example System Architecture

FIG. **1** is a block diagram of a data subject access request processing and fulfillment system **100** according to a particular embodiment. In various embodiments, the data subject access request processing and fulfillment system is part of a privacy compliance system (also referred to as a privacy management system), or other system, which may, for example, be associated with a particular organization and be configured to aid in compliance with one or more legal or industry regulations related to the collection and storage of personal data.

As may be understood from FIG. **1**, the data subject access request processing and fulfillment system **100** includes one or more computer networks **115**, a Data Model Generation Server **110**, a Data Model Population Server **120**, an Intelligent Identity Scanning Server **130** (which may automatically validate a DSAR requestor's identity), One or More Databases **140** or other data structures, one or more remote computing devices **150** (e.g., a desktop computer, laptop computer, tablet computer, smartphone, etc.), and One or More Third Party Servers **160**. In particular embodiments, the one or more computer networks **115** facilitate communication between the Data Model Generation Server

110, Data Model Population Server 120, Intelligent Identity Scanning/Verification Server 130, One or More Databases 140, one or more remote computing devices 150 (e.g., a desktop computer, laptop computer, tablet computer, smartphone, etc.), One or More Third Party Servers 160, and DSAR Processing and Fulfillment Server 170. Although in the embodiment shown in FIG. 1, the Data Model Generation Server 110, Data Model Population Server 120, Intelligent Identity Scanning Server 130, One or More Databases 140, one or more remote computing devices 150 (e.g., a desktop computer, laptop computer, tablet computer, smartphone, etc.), and One or More Third Party Servers 160, and DSAR Processing and Fulfillment Server 170 are shown as separate servers, it should be understood that in other embodiments, the functionality of one or more of these servers and/or computing devices may, in different embodiments, be executed by a larger or smaller number of local servers, one or more cloud-based servers, or any other suitable configuration of computers.

The one or more computer networks 115 may include any of a variety of types of wired or wireless computer networks such as the Internet, a private intranet, a public switch telephone network (PSTN), or any other type of network. The communication link between the DSAR Processing and Fulfillment Server 170 and the One or More Remote Computing Devices 150 may be, for example, implemented via a Local Area Network (LAN) or via the Internet. In other embodiments, the One or More Databases 140 may be stored either fully or partially on any suitable server or combination of servers described herein.

FIG. 2A illustrates a diagrammatic representation of a computer 200 that can be used within the data subject access request processing and fulfillment system 100, for example, as a client computer (e.g., one or more remote computing devices 150 shown in FIG. 1), or as a server computer (e.g., Data Model Generation Server 110 shown in FIG. 1). In particular embodiments, the computer 200 may be suitable for use as a computer within the context of the data subject access request processing and fulfillment system 100 that is configured for routing and/or processing DSAR requests and/or generating one or more data models used in automatically fulfilling those requests.

In particular embodiments, the computer 200 may be connected (e.g., networked) to other computers in a LAN, an intranet, an extranet, and/or the Internet. As noted above, the computer 200 may operate in the capacity of a server or a client computer in a client-server network environment, or as a peer computer in a peer-to-peer (or distributed) network environment. The Computer 200 may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a server, a network router, a switch or bridge, or any other computer capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that computer. Further, while only a single computer is illustrated, the term "computer" shall also be taken to include any collection of computers that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

An exemplary computer 200 includes a processing device 202, a main memory 204 (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) such as synchronous DRAM (SDRAM) or Rambus DRAM (RDRAM), etc.), static memory 206 (e.g., flash memory, static random access memory (SRAM), etc.), and a data storage device 218, which communicate with each other via a bus 232.

The processing device 202 represents one or more general-purpose processing devices such as a microprocessor, a central processing unit, or the like. More particularly, the processing device 202 may be a complex instruction set computing (CISC) microprocessor, reduced instruction set computing (RISC) microprocessor, very long instruction word (VLIW) microprocessor, or processor implementing other instruction sets, or processors implementing a combination of instruction sets. The processing device 202 may also be one or more special-purpose processing devices such as an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a digital signal processor (DSP), network processor, or the like. The processing device 202 may be configured to execute processing logic 226 for performing various operations and steps discussed herein.

The computer 120 may further include a network interface device 208. The computer 200 also may include a video display unit 210 (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)), an alphanumeric input device 212 (e.g., a keyboard), a cursor control device 214 (e.g., a mouse), and a signal generation device 216 (e.g., a speaker).

The data storage device 218 may include a non-transitory computer-accessible storage medium 230 (also known as a non-transitory computer-readable storage medium or a non-transitory computer-readable medium) on which is stored one or more sets of instructions (e.g., software instructions 222) embodying any one or more of the methodologies or functions described herein. The software instructions 222 may also reside, completely or at least partially, within main memory 204 and/or within processing device 202 during execution thereof by computer 200—main memory 204 and processing device 202 also constituting computer-accessible storage media. The software instructions 222 may further be transmitted or received over a network 115 via network interface device 208.

While the computer-accessible storage medium 230 is shown in an exemplary embodiment to be a single medium, the term "computer-accessible storage medium" should be understood to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The terms "computer-accessible storage medium", "computer-readable medium", and like terms should also be understood to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the computer and that cause the computer to perform any one or more of the methodologies of the present invention. These terms should accordingly be understood to include, but not be limited to, solid-state memories, optical and magnetic media, etc.

Systems for Managing Data Subject Access Requests

In various embodiments, the system may include a ticket management system and/or other systems for managing data subject access requests. In operation, the system may use one or more computer processors, which are operatively coupled to memory, to execute one or more software modules (which may be included in the Instructions 222 referenced above) such as: (1) a DSAR Request Routing Module 1000; and (4) a DSAR Prioritization Module. An overview of the functionality and operation of each of these modules is provided below.

Data Subject Access Request Routing Module 1000

As shown in FIG. 2B, a Data Subject Access Request Routing Module 1000, according to particular embodiments,

is adapted for executing the steps of: (1) at Step **1050**, presenting, by at least one computer processor, a first webform on a first website, the first webform being adapted to receive data subject access requests and to route the requests to a first designated individual (e.g., an individual who is associated with a first sub-organization of a particular organization—e.g., an employee of the first sub-organization) for processing (in various embodiments, "presenting a webform on a website" may comprise, for example: (A) providing a button, link, or other selectable indicium on the website that, when selected, causes the system to display the webform, or (B) displaying the webform directly on the website); (2) at Step **1100** presenting, by at least one computer processor, a second webform on a second website, the second webform being adapted to receive data subject access requests and to route the requests to a second designated individual (e.g., an individual who is associated with a second sub-organization of a particular organization—e.g., an employee of the second sub-organization) for processing; (3) at Step **1150**, receiving, by at least one computer processor, via the first webform, a first data subject access request; (4) at Step **1200**, at least partially in response to the receiving the first data subject access request, automatically routing the first data subject access request to the first designated individual for handling; (5) at Step **1250**, at least partially in response to the receiving the second data subject access request, automatically routing the second data subject access request to the second designated individual for handling; and (6) at Step **1300**, communicating, via a single user interface, a status of both the first data subject access request and the second data subject access request.

In particular embodiments: (1) the first website is a website of a first sub-organization of a particular parent organization; (2) the second website is a website of a second sub-organization of the particular parent organization; and (3) the computer-implemented method further comprises communicating, by at least one computer processor, via a single user interface, a status of each of said first data subject access request and said second data subject access request (e.g., to an employee of—e.g., privacy officer of—the parent organization). As discussed in more detail below, this single user interface may display an indication, for each respective one of the first and second data subject access requests, of a number of days remaining until a deadline for fulfilling the respective data subject access request.

In certain embodiments, the single user interface is adapted to facilitate the deletion or assignment of multiple data subject access requests to a particular individual for handling in response to a single command from a user (e.g., in response to a user first selecting multiple data subject access requests from the single user interface and then executing an assign command to assign each of the multiple requests to a particular individual for handling).

In particular embodiments, the system running the Data Subject Access Request Routing Module **1000**, according to particular embodiments, may be adapted for, in response to receiving each data subject access request, generating an ID number (e.g., a transaction ID or suitable Authentication Token) for the first data subject access request, which may be used later, by the DSAR requestor, to access information related to the DSAR, such as personal information requested via the DSAR, the status of the DSAR request, etc. To facilitate this, the system may be adapted for receiving the ID number from an individual and, at least partially in response to receiving the ID number from the individual, providing the individual with information regarding status of the data subject access request and/or information previously requested via the data subject access request.

In particular embodiments, the system may be adapted to facilitate the processing of multiple different types of data subject access requests. For example, the system may be adapted to facilitate processing: (1) requests for all personal data that an organization is processing for the data subject (a copy of the personal data in a commonly used, machine-readable format); (2) requests for all such personal data to be deleted; (3) requests to update personal data that the organization is storing for the data subject; (4) requests to opt out of having the organization use the individual's personal information in one or more particular ways (e.g., per the organization's standard business practices), or otherwise change the way that the organization uses the individual's personal information; and/or (5) the filing of complaints.

In particular embodiments, the system may execute one or more steps (e.g., any suitable step or steps discussed herein) automatically. For example, the system may be adapted for: (1) receiving, from the first designated individual, a request to extend a deadline for satisfying the first data subject access request; (2) at least partially in response to receiving the extension request, automatically determining, by at least one processor, whether the requested extension complies with one or more applicable laws or internal policies; and (3) at least partially in response to determining that the requested extension complies with the one or more applicable laws or internal policies, automatically modifying the deadline, in memory, to extend the deadline according to the extension request. The system may be further adapted for, at least partially in response to determining that the requested extension does not comply with the one or more applicable laws or internal policies, automatically rejecting the extension request. In various embodiments, the system may also, or alternatively, be adapted for: (1) at least partially in response to determining that the requested extension does not comply with the one or more applicable laws or internal policies, automatically modifying the length of the requested extension to comply with the one or more applicable laws or internal policies; and (2) automatically modifying the deadline, in memory, to extend the deadline according to the extension request.

In various embodiments, the system may be adapted for: (1) automatically verifying an identity of a particular data subject access requestor placing the first data subject access request; (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically obtaining, from a particular data model, at least a portion of information requested in the first data subject access request; and (3) after obtaining the at least a portion of the requested information, displaying the obtained information to a user as part of a fulfillment of the first data subject access request. The information requested in the first data subject access request may, for example, comprise at least substantially all (e.g., most or all) of the information regarding the first data subject that is stored within the data model.

In various embodiments, the system is adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor placing the first data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically facilitating an update of personal data that an organization associated with the first webform is processing regarding the particular data subject access requestor.

Similarly, in particular embodiments, the system may be adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor placing the first data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically processing a request, made by the particular data subject access requestor, to opt out of having the organization use the particular data subject access requestor's personal information in one or more particular ways.

The system may, in various embodiments, be adapted for: (1) providing, by at least one computer processor, a webform creation tool that is adapted for receiving webform creation criteria from a particular user, the webform creation criteria comprising at least one criterion from a group consisting of: (A) a language that the form will be displayed in; (B) what information is to be requested from data subjects who use the webform to initiate a data subject access request; and (C) who any data subject access requests that are received via the webform will be routed to; and (2) executing the webform creation tool to create both the first webform and the second webform.

In light of the discussion above, although the Data Subject Access Request Routing Module **1000** is described as being adapted to, in various embodiments, route data subject access requests to particular individuals for handling, it should be understood that, in particular embodiments, this module may be adapted to process at least part of, or all of, particular data subject access requests automatically (e.g., without input from a human user). In such cases, the system may or may not route such automatically-processed requests to a designated individual for additional handling or monitoring. In particular embodiments, the system may automatically fulfill all or a portion of a particular DSAR request, automatically assign a transaction ID and/or authentication token to the automatically fulfilled transaction, and then display the completed DSAR transaction for display on a system dashboard associated with a particular responsible individual that would otherwise have been responsible for processing the DSAR request (e.g., an individual to whom the a webform receiving the DSAR would otherwise route DSAR requests). This may be helpful in allowing the human user to later track, and answer any questions about, the automatically-fulfilled DSAR request.

It should also be understood that, although the system is described, in various embodiments, as receiving DSAR requests via multiple webforms, each of which is located on a different website, the system may, in other embodiments, receive requests via only a single webform, or through any other suitable input mechanism other than a webform (e.g., through any suitable software application, request via SMS message, request via email, data transfer via a suitable API, etc.)

In various embodiments, the system may be adapted to access information needed to satisfy DSAR requests via one or more suitable data models. Such data models include those that are described in greater detail in U.S. patent application Ser. No. 15/996,208, filed Jun. 1, 2018, which, as noted above, is incorporated herein by reference. In various embodiments, the system is adapted to build and access such data models as described in this earlier-filed U.S. patent application.

As an example, in fulfilling a request to produce, modify, or delete, any of a data subject's personal information that is stored by a particular entity, the system may be adapted to access a suitable data model to identify any personal data of the data subject that is currently being stored in one or more computer systems associated with the particular entity. After using the data model to identify the data, the system may automatically process the data accordingly (e.g., by modifying or deleting it, and/or sharing it with the DSAR requestor).

DSAR Prioritization Module

A DSAR Prioritization Module, according to various embodiments, is adapted for (1) executing the steps of receiving a data subject access request; (2) at least partially in response to receiving the data subject access request, obtaining metadata regarding a data subject of the data subject access request; (3) using the metadata to determine whether a priority of the DSAR should be adjusted based on the obtained metadata; and (4) in response to determining that the priority of the DSAR should be adjusted based on the obtained metadata, adjusting the priority of the DSAR.

The operation of various embodiments of the various software modules above is described in greater detail below. It should be understood that the various steps described herein may be executed, by the system, in any suitable order and that various steps may be omitted, or other steps may be added in various embodiments.

Operation of Example Implementation

FIGS. **3-43** are screen shots that demonstrate the operation of a particular embodiment. FIGS. **3-6** show a graphical user interface (GUI) of an example webform construction tool. FIG. **3** shows a user working to design a webform called "Web_form_**1**". As may be understood from the vertical menu shown on the left-hand side of the screen, the webform construction tool allows users to design a webform by: (1) specifying the details of the form (via the "Form Details" tab); (2) defining the fields that will be displayed on the webform (via the "Webform Fields" tab); (3) defining the styling of the webform (via the "Form Styling" tab); and (4) defining various settings associated with the webform (via the "Settings" tab). As shown in FIGS. **4-6**, the user may also specify text to be displayed on the webform (e.g., via a "Form Text" tab).

FIG. **4** shows that, by selecting the "Form Details" tab, the user may define which answers a requestor will be able to specify on the webform in response to prompts for information regarding what type of individual they are (customer, employee, etc.) and what type of request they are making via the webform. Example request types include: (1) a request for all personal data that an organization is processing for the data subject (a copy of the personal data in a commonly used, machine-readable format); (2) a request for all such personal data to be deleted; (3) a request to update personal data that the organization is storing for the data subject; (4) a request to opt out of having the organization use the individual's personal information in one or more particular ways (e.g., per the organization's standard business practices); (5) file a complaint; and/or (6) other.

FIG. **5** shows that, by selecting the "Settings" tab, the user may specify various system settings, such as whether Captcha will be used to verify that information is being entered by a human, rather than a computer.

FIG. **6** shows that, by selecting the Form Styling tab, the user may specify the styling of the webform. The styling may include, for example: (1) a header logo; (2) header height; (3) header color; (4) body text color; (5) body text size; (6) form label color; (7) button color; (8) button text color; (9) footer text color; (10) footer text size; and/or any other suitable styling related to the webform.

In other embodiments, the system is configured to enable a user to specify, when configuring a new webform, what individual at a particular organization (e.g., company) will

be responsible for responding to requests made via the webform. The system may, for example, enable the user to define a specific default sub-organization (e.g., within the organization) responsible for responding to DSAR's submitted via the new webform. As such, the system may be configured to automatically route a new DSAR made via the new webform to the appropriate sub-organization for processing and fulfillment. In various embodiments, the system is configured to route one or more various portions of the DSAR to one or more different sub-organizations within the organization for handling.

In particular embodiments, the system may include any suitable logic for determining how the webform routes data subject access requests. For example, the system may be adapted to determine which organization or individual to route a particular data subject access request to based, at least in part, on one or more factors selected from a group consisting of: (1) the data subject's current location; (2) the data subject's country of residence; (3) the type of request being made; (4) the type of systems that contain (e.g., store and/or process) the user's personal data (e.g., in ADP, Salesforce, etc.); or any other suitable factor.

In particular embodiments, the system is configured to enable a user generating webforms to assign multiple webforms to multiple different respective suborganizations within an organization. For example, an organization called ACME, Inc. may have a website for each of a plurality of different brands (e.g., sub-organizations) under which ACME sells products (e.g., UNICORN Brand T-shirts, GRIPP Brand Jeans, etc.). As may be understood in light of this disclosure, each website for each of the particular brands may include an associated webform for submitting DSAR's (either a webform directly on the web site, or one that is accessible via a link on the website). Each respective webform may be configured to route a DSAR made via its associated brand website to a particular sub-organization and/or individuals within ACME for handling DSAR's related to the brand.

As noted above, after the user uses the webform construction tool to design a particular webform for use on a particular web page, the webform construction tool generates code (e.g., HTML code) that may be pasted into the particular web page to run the designed webform page. In particular embodiment, when pasted into the particular web page, the code generates a selectable button on the web page that, when selected, causes the system to display a suitable DSAR request webform.

FIG. **7** shows the privacy webpage of a company (e.g., the ACME corporation). As shown in this figure, a requestor may submit a DSAR by selecting a "Submit a Privacy Related Request" button on the web page.

FIG. **8** shows a webform that is displayed after a requestor selects the "Submit a Privacy Related Request" button on the privacy webpage of FIG. **7**. As may be understood from this figure, the requestor may complete the webform by specifying which type of user they are, and what type of request they are making. The webform also asks the requestor to provide enough personal information to confirm their identity (e.g., and fulfill the request). As shown in this figure, the system may prompt a user submitting a DSAR to provide information for the user such as, for example: (1) what type of requestor the user is (e.g., employee, customer, etc.); (2) what the request involves (e.g., requesting info, opting out, deleting data, updating data, etc.); (3) first name; (4) last name; (5) email address; (6) telephone number; (7) home address; (8) one or more other pieces of identifying information; and/or (9) one or more details associated with the request. FIG. **9** shows an example populated version of the webform.

As shown in FIG. **10**, after a requestor completes the webform and selects a "submit" indicia, the system displays a message to the requestor indicating that their DSAR has been successfully submitted. The system also displays a Request ID associated with the request. In response to the requestor successfully submitting the request, the system may also send an email (or other suitable communication) to the requestor confirming the request. An example of a suitable confirmation email is shown in FIG. **11**.

In various embodiments, the system includes a dashboard that may be used by various individuals within an organization (e.g., one or more privacy officers of an organization) to manage multiple DSAR requests. As discussed above, the dashboard may display DSAR's submitted, respectively, to a single organization, any of multiple different sub-organizations (divisions, departments, subsidiaries etc.) of a particular organization, and/or any of multiple independent organizations. For example, the dashboard may display a listing of DSAR's that were submitted from a parent organization and from the parent organization's U.S. and European subsidiaries. This may be advantageous, for example, because it may allow an organization to manage all DSAR requests of all of its sub-organizations (and/or other related organizations) centrally.

FIGS. **12-23**, **25-27**, **29-34**, and **41-43** depict various example user-interface screens of a DSAR request-management dashboard. As may be understood from FIG. **12**, after an appropriate user (e.g., a privacy officer associated with a particular organization) logs into the system, the system may display a Data Subject Request Queue that may, for example, display a listing of all data subject access requests that the appropriate individual has been designated to process. As shown in FIG. **12**, each data subject access request may be represented by a respective row of information that includes: (1) an ID number for the request; (2) the name of the data subject who has submitted the request; (3) the status of the request; (4) the number of days that are left to respond to the request (e.g., according to applicable laws and/or internal procedures); (5) an indication as to whether the deadline to respond to the request has been extended; (6) a creation date of the request; (7) an indication of the type of requestor that submitted the request (customer, employee, etc.); (8) the name of the individual who has been assigned to process the request (e.g., the respondent). This screen may also include selectable "Edit" and "Filter" buttons that respectively facilitate acting on and filtering the various requests displayed on the page.

As shown in FIG. **13**, in response to a respondent selecting the edit button while a particular DSAR is highlighted, the system displays a dropdown menu allowing the respondent to select between taking the following actions: (1) verify the request; (2) assign the request to another individual; (3) request an extension; (4) reject the request; or (5) suspend the request.

FIGS. **14** and **15** show a message that the system displays to the respondent in response to the respondent selecting the "verify" option. As shown in this figure, the system prompts the respondent to indicate whether they are sure that they wish to authenticate the request. The system also presents an input field where the respondent can enter text to be displayed to the requestor along with a request for the requestor to provide information verifying that they are the data

subject associated with the request. After the respondent populates the input field, they may submit the request by selecting a "Submit" button.

In particular embodiments, the input field may enable the respondent to provide one or more supporting reasons for a decision, by the respondent, to authenticate the request. The respondent may also upload one or more supporting documents (such as an attachment). The supporting documents or information may include, for example, one or more documents utilized in confirming the requestor's identity, etc.

In response to the respondent selecting the Submit button, the system changes the status of the request to "In Progress" and also changes the color of the request's status from orange to blue (or from any other suitable color to any different suitable color)—see FIG. **16**. The system also generates and sends a message (e.g., an electronic or paper message) to the requestor asking them to submit information verifying the request. The message may include the text that the respondent entered in the text box of FIG. **14**.

As shown in FIGS. **17-19**, in response to a respondent selecting the "Edit" button and then selecting the "Assign" indicia from the displayed dropdown menu, the system displays a Request Assignment interface that allows a respondent to indicate who the request should be assigned to. For example, the respondent may indicate that they will be handling the request, or assign the request to another suitable individual, who may, for example, then be designated as the respondent for the request. If the respondent assigns the request to another individual for handling, the respondent may also provide an email address or other correspondence information for the individual. The Request Assignment interface includes a comment box for allowing a respondent to add a message to the individual that the assignment will be assigned to regarding the assignment. In response to the respondent selecting the "Assign" button, the system assigns the request to the designated individual for handling. If the request has been assigned to another, designated individual, the system automatically generates and sends a message (e.g., an electronic message such as an email or SMS message) to the designated individual informing them of the assignment.

As shown in FIGS. **20-22**, in response to a respondent selecting the "Edit" button and then selecting the "Reject" indicia from the displayed dropdown menu, the system displays a Reject Request interface. This interface includes a comment box for allowing a respondent to add a message to the requestor as to why the request was rejected. In response to the respondent selecting the "Submit" button, the system changes the status of the request to "Rejected" and changes the color of the request's status indicator to red (See FIG. **23**). The system may also automatically generate a message (e.g., an electronic or paper message) to the requestor notifying them that their request has been rejected and displaying the text that the respondent entered into the Reject Request interface of FIG. **22**. An example of such a message is shown in FIG. **24**.

As shown in FIGS. **25-26**, in response to a respondent selecting the "Edit" button and then selecting the "Request Extension" indicia from the displayed dropdown menu, the system displays a Request Extension interface. This includes a text box for allowing a user to indicate the number of days for which they would like to extend the current deadline for responding to the request. For example, the dialog box of FIG. **26** shows the respondent requesting that the current deadline be extended by 90 days. In response to the respondent entering a desired extension duration and selecting the "Submit" button, the system updates the deadline in the system's memory (e.g., in an appropriate data structure) to reflect the extension. For instance, in the example of FIG. **26**, the system extends the deadline to be 90 days later than the current deadline. As shown in FIG. **27**, the system also updates the "Days Left to Respond" field within the Data Subject Request Queue to reflect the extension (e.g., from 2 days from the current date to 92 days from the current date). As shown in FIG. **28**, the system may also generate an appropriate message (e.g., an electronic, such as an email, or a paper message) to the requestor indicating that the request has been delayed. This message may provide a reason for the delay and/or an anticipated updated completion date for the request.

In particular embodiments, the system may include logic for automatically determining whether a requested extension complies with one or more applicable laws or internal policies and, in response, either automatically grant or reject the requested extension. For example, if the maximum allowable time for replying to a particular request is 90 days under the controlling laws and the respondent requests an extension that would result in the fulfillment of the request 91 or more days from the date that the request was submitted, the system may automatically reject the extension request. In various embodiments, the system may also communicate, to the respondent (e.g., via a suitable electronic message or text display on a system user interface) an explanation as to why the extension request was denied, and/or a maximum amount of time (e.g., a maximum number of days) that the deadline may be extended under the applicable laws or policies. In various embodiments, if the system determines that the requested extension is permissible under the applicable laws and/or policies, the system may automatically grant the extension.

In other embodiments, the system may be configured to automatically modify a length of the requested extension to conform with one or more applicable laws and/or policies. For example, if the request was for a 90-day extension, but only a 60 day extension is available under the applicable laws or regulations, the system may automatically grant a 60-day extension rather than a 90 day extension. The system may be adapted to also automatically generate and transmit a suitable message (e.g., a suitable electronic or paper communication) notifying them of the fact that the extension was granted for a shorter, specified period of time than requested.

As shown in FIGS. **29-34**, a respondent may obtain additional details regarding a particular request by selecting (e.g., clicking on) the request on the Data Subject Request Queue screen. For example, FIG. **30** shows a Data Subject Request Details screen that the system displays in response to a respondent selecting the "Donald Blair" request on the user interface screen of FIG. **35**. As shown in FIG. **30**, the Data Subject Request Details screen shows all correspondence between the organization and the requesting individual regarding the selected data subject access request. As may be understood from FIG. **31**, when a respondent selects a particular correspondence (e.g., email), the system displays the correspondence to the respondent for review or other processing.

As shown in FIG. **32**, in various embodiments, the system may provide a selectable "Reply" indicia that allows the respondent to reply to particular correspondence from an individual. As may be understood from this figure, in response to the respondent selecting the "Reply" indicia, the system may display a dropdown menu of various standard replies. For example, the dropdown menu may provide the option of generating a reply to the requestor indicating that

the request has been rejected, is pending, has been extended, or that the request has been completed.

As shown in FIG. **33**, in response to the respondent selecting "Reply as Completed", the system may generate a draft email to the requestor explaining that the request has been completed. The respondent may then edit this email and send the edited correspondence (e.g., via email) to the requestor by selecting a "Send as Complete" indicia. As shown in FIG. **34**, the system may, in response, display an indicator adjacent the correspondence indicating that the correspondence included a reply indicating that the request was complete. This may be useful in allowing individuals to understand the contents of the correspondence without having to open it.

FIG. **35** shows an example email automatically generated by the system in response to the respondent selecting "Reply as Completed" on the screen shown in FIG. **32**. As shown in FIG. **35**, the correspondence may include a secure link that the requestor may select to access the data that was requested in the DSAR. In particular embodiments, the link is a link to a secure website, such as the website shown in FIG. **36**, that provides access to the requested data (e.g., by allowing a user to download a .pdf file, or other suitable file, that includes the requested data). As shown in FIG. **36**, the website may require multiple pieces of data to verify that the requestor is permitted to access the site. For example, in order to access the website, the requestor may be required to provide both the unique ID number of the request, and an authentication token, which the system may send to the user via email—See FIGS. **37** and **38**.

FIGS. **39-43** are computer screen shots that depict additional user interfaces according to various embodiments.

Additional Concepts

Intelligent Prioritization of DSAR's

In various embodiments, the system may be adapted to prioritize the processing of DSAR's based on metadata about the data subject of the DSAR. For example, the system may be adapted for: (1) in response to receiving a DSAR, obtaining metadata regarding the data subject; (2) using the metadata to determine whether a priority of the DSAR should be adjusted based on the obtained metadata; and (3) in response to determining that the priority of the DSAR should be adjusted based on the obtained metadata, adjusting the priority of the DSAR.

Examples of metadata that may be used to determine whether to adjust the priority of a particular DSAR include: (1) the type of request, (2) the location from which the request is being made, (3) current sensitivities to world events, (4) a status of the requestor (e.g., especially loyal customer), or (5) any other suitable metadata.

In various embodiments, in response to the system determining that the priority of a particular DSAR should be elevated, the system may automatically adjust the deadline for responding to the DSAR. For example, the system may update the deadline in the system's memory and/or modify the "Days Left to Respond" field (See FIG. **13**) to include a fewer number of days left to respond to the request. Alternatively, or in addition, the system may use other techniques to convey to a respondent that the request should be expedited (e.g., change the color of the request, send a message to the respondent that they should process the request before non-prioritized requests, etc.)

In various embodiments, in response to the system determining that the priority of a particular DSAR should be lowered, the system may automatically adjust the deadline for responding to the DSAR by adding to the number of days left to respond to the request.

Automatic Deletion of Data Subject Records Based on Detected Systems

In particular embodiments, in response a data subject submitting a request to delete their personal data from an organization's systems, the system may: (1) automatically determine where the data subject's personal data is stored; and (2) in response to determining the location of the data (which may be on multiple computing systems), automatically facilitate the deletion of the data subject's personal data from the various systems (e.g., by automatically assigning a plurality of tasks to delete data across multiple business systems to effectively delete the data subject's personal data from the systems). In particular embodiments, the step of facilitating the deletion may comprise, for example: (1) overwriting the data in memory; (2) marking the data for overwrite; (2) marking the data as free (e.g., and deleting a directory entry associated with the data); and/or (3) any other suitable technique for deleting the personal data. In particular embodiments, as part of this process, the system uses an appropriate data model (see discussion above) to efficiently determine where all of the data subject's personal data is stored.

Automatic Determination of Business Processes that Increase Chance of Deletion Requests

In various embodiments, the system is adapted to store, in memory, a log of DSAR actions. The system may also store, in memory, additional information regarding the data subjects of each of the requests. The system may use this information, for example, to determine which business processes are most commonly associated with a data subject submitting a request to have their personal information deleted from the organization's systems. The organization may then use this information to revise the identified business processes in an effort to reduce the number of deletion requests issued by data subjects associated with the business processes.

As a particular example, the system may analyze stored information to determine that a high number (e.g., 15%) of all participants in a company's loyalty program submit requests to have their personal information deleted from the company's systems. In response to making this determination, the system may issue an electronic alert to an appropriate individual (e.g., a privacy officer of the company), informing them of the high rate of members of the company's loyalty program issuing personal data delete requests. This alert may prompt the individual to research the issue and try to resolve it.

Automated Data Subject Verification

In various embodiments, before a data subject request can be processed, the data subject's identity may need to be verified. In various embodiments, the system provides a mechanism to automatically detect the type of authentication required for a particular data subject based on the type of Data Subject Access Request being made and automatically issues a request to the data subject to verify their identity against that form of identification. For example, a subject rights request might only require two types of authentication, but a deletion request may require four types of data to verify authentication. The system may automatically detect which is type of authentication is required based on the DSAR and send an appropriate request to the data subject to verify their identity.

Stated more particularly, when processing a data subject access request, the system may be configured to verify an identity of the data subject prior to processing the request (e.g., or as part of the processing step). In various embodiments, confirming the identity of the data subject may, for

example, limit a risk that a third-party or other entity may gain unlawful or unconsented to access to the requestor's personal data. The system may, for example, limit processing and fulfillment of requests relating to a particular data subject to requests that are originated by (e.g., received from) the particular data subject. When processing a data subject access request, the system may be configured to use various reasonable measures to verify the identity of the data subject who requests access (e.g., in particular in the context of online services and online identifiers). In particular embodiments, the system is configured to substantially automatically validate an identity of a data subject when processing the data subject access request.

For example, in particular embodiments, the system may be configured to substantially automatically (e.g., automatically) authenticate and/or validate an identity of a data subject using any suitable technique. These techniques may include, for example: (1) one or more credit-based and/or public- or private-information-based verification techniques; (2) one or more company verification techniques (e.g., in the case of a business-to-business data subject access request); (3) one or more techniques involving integration with a company's employee authentication system; (4) one or more techniques involving a company's (e.g., organization's) consumer portal authentication process; (5) etc. Various exemplary techniques for authenticating a data subject are discussed more fully below.

In particular embodiments, when authenticating a data subject (e.g., validating the data subject's identity), the system may be configured to execute particular identity confirmation steps, for example, by interfacing with one or more external systems (e.g., one or more third-party data aggregation systems). For example, the system, when validating a data subject's identity, may begin by verifying that a person with the data subject's name, address, social security number, or other identifying characteristic (e.g., which may have been provided by the data subject as part of the data subject access request) actually exists. In various embodiments, the system is configured to interface with (e.g., transmit a search request to) one or more credit reporting agencies (e.g., Experian, Equifax, TransUnion, etc.) to confirm that a person with one or more characteristics provided by the data subject exists. The system may, for example, interface with such credit reporting agencies via a suitable plugin (e.g., software plugin). Additionally, there might be a verification on behalf of a trusted third-party system (e.g., the controller).

In still other embodiments, the system may be configured to utilize one or more other third-party systems (e.g., such as LexisNexis, IDology, RSA, etc.), which may, for example, compile utility and phone bill data, property deeds, rental agreement data, and other public records for various individuals. The system may be configured to interface with one or more such third-party systems to confirm that a person with one or more characteristics provided by the data subject exists.

After the step of confirming the existence of a person with the one or more characteristics provided by the data subject, the system may be configured to confirm that the person making the data subject access request is, in fact, the data subject. The system may, for example, verify that the requestor is the data subject by prompting the requestor to answer one or more knowledge-based authentication questions (e.g., out-of-wallet questions). In particular embodiments, the system is configured to utilize one or more third-party services as a source of such questions (e.g., any of the suitable third-party sources discussed immediately above). The system may use third-party data from the one or more third-party sources to generate one or more questions. These one or more questions may include questions that a data subject should know an answer to without knowing the question ahead of time (e.g., one or more previous addresses, a parent or spouse name and/or maiden name, etc.).

FIG. **46** depicts an exemplary identity verification questionnaire. As may be understood from this figure, an identity verification questionnaire may include one or more questions whose responses include data that the system may derive from one or more credit agencies or other third-party data aggregation services (e.g., such as previous street addresses, close associates, previous cities lived in, etc.). In particular embodiments, the system is configured to provide these one or more questions to the data subject in response to receiving the data subject access request. In other embodiments, the system is configured to prompt the data subject to provide responses to the one or more questions at a later time (e.g., during processing of the request). In particular other embodiments, the system is configured to substantially automatically compare one or more pieces of information provided as part of the data subject access request to one or more pieces of data received from a third-party data aggregation service in order to substantially automatically verify the requestor's identity.

In still other embodiments, the system may be configured to prompt a requestor to provide one or more additional pieces of information in order to validate the requestor's identity. This information may include, for example: (1) at least a portion of the requestor's social security number (e.g., last four digits); (2) a name and/or place of birth of the requestor's father; (3) a name, maiden name, and/or place of birth of the requestor's mother; and/or (4) any other information which may be useful for confirming the requestor's identity (e.g., such as information available on the requestor's birth certificate). In other embodiments, the system may be configured to prompt the requestor to provide authorization for the company to check the requestor's social security or other private records (e.g., credit check authorization, etc.) to obtain information that the system may use to confirm the requestor's identity. In other embodiments, the system may prompt the user to provide one or more images (e.g., using a suitable mobile computing device) of an identifying document (e.g., a birth certificate, social security card, driver's license, etc.).

The system may, in response to a user providing one or more responses that matches information that the system receives from one or more third-party data aggregators or through any other suitable background, credit, or other search, substantially automatically authenticate the requestor as the data subject. The system may then continue processing the data subject's request, and ultimately fulfill their request.

In particular embodiments, such as embodiments in which the requestor includes a business (e.g., as in a business to business data subject access request), the system may be configured to authenticate the requesting business using one or more company verification techniques. These one or more company validation techniques may include, for example, validating a vendor contract (e.g., between the requesting business and the company receiving the data subject access request); receiving a matching token, code, or other unique identifier provided by the company receiving the data subject access request to the requesting business; receiving a matching file in possession of both the requesting business and the company receiving the data subject access request;

receiving a signed contract, certificate (e.g., digital or physical), or other document memorializing an association between the requesting business and the company receiving the data subject access request; and/or any other suitable method of validating that a particular request is actually made on behalf of the requesting business (e.g., by requesting the requesting business to provide one or more pieces of information, one or more files, one or more documents, etc. that may only be accessible to the requesting business).

In other embodiments, the system may be configured to authenticate a request via integration with a company's employee or customer (e.g., consumer) authentication process. For example, in response to receiving a data subject access request that indicates that the data subject is an employee of the company receiving the data subject access request, the system may be configured to prompt the employee to login to the company's employee authentication system (e.g., Okta, Azure, AD, etc.) In this way, the system may be configured to authenticate the requestor based at least in part on the requestor successfully logging into the authentication system using the data subject's credentials. Similarly, in response to receiving a data subject access request that indicates that the data subject is a customer of the company receiving the data subject access request, the system may be configured to prompt the customer to login to an account associated with the company (e.g., via a consumer portal authentication process). In a particular example, this may include, for example, an Apple ID (for data subject access requests received by Apple). In this way, the system may be configured to authenticate the requestor based at least in part on the requestor successfully logging into the authentication system using the data subject's credentials. In some embodiments, the system may be configured to require the requestor to login using two-factor authentication or other suitable existing employee or consumer authentication process.

Data Subject Blacklist

In various embodiments, a particular organization may not be required to respond to a data subject access request that originates (e.g., is received from) a malicious requestor. A malicious requestor may include, for example: (1) a requestor (e.g., an individual) that submits excessive or redundant data subject access requests; (2) a group of requestors such as researchers, professors, students, NGOs, etc. that submit a plurality of requests for reasons other than those reasons provided by policy, law, etc.; (3) a competitor of the company receiving the data subject access request that is submitting such requests to tie up the company's resources unnecessarily; (4) a terrorist or other organization that may spam requests to disrupt the company's operation and response to valid requests; and/or (5) any other request that may fall outside the scope of valid requests made for reasons proscribed by public policy, company policy, or law. In particular embodiments, the system is configured to maintain a blacklist of such malicious requestors.

In particular embodiments, the system is configured to track a source of each data subject access request and analyze each source to identify sources from which: (1) the company receives a large volume of requests; (2) the company receives a large number of repeat requests; (3) etc. These sources may include, for example: (1) one or more particular IP addresses; (2) one or more particular domains; (3) one or more particular countries; (4) one or more particular institutions; (5) one or more particular geographic regions; (6) etc. In various embodiments, in response to analyzing the sources of the requests, the system may identify one or more sources that may be malicious (e.g., are submitting excessive requests).

In various embodiments, the system is configured to maintain a database of the identified one or more sources (e.g., in computer memory). In particular embodiments, the database may store a listing of identities, data sources, etc. that have been blacklisted (e.g., by the system). In particular embodiments, the system is configured to, in response to receiving a new data subject access request, cross reference the request with the blacklist to determine if the requestor is on the blacklist or is making the request from a blacklisted source. The system may then, in response to determining that the requestor or source is blacklisted, substantially automatically reject the request. In particular embodiments, the blacklist cross-referencing step may be part of the requestor authentication (e.g., verification) discussed above. In various embodiments, the system may be configured to analyze request data on a company by company basis to generate a blacklist. In other embodiments, the system may analyze global data (e.g., all data collected for a plurality of companies that utilize the data subject access request fulfillment system) to generate the blacklist.

In particular embodiments, the system may be configured to fulfill data subject access requests for the purpose of providing a data subject with information regarding what data the company collects and for what purpose, for example, so the data subject can ensure that the company is collecting data for lawful reasons. As such, the system may be configured to identify requestors and other sources of data requests that are made for other reasons (e.g., one or more reasons that would not obligate the company to respond to the request). These reasons may include, for example, malicious or other reasons such as: (1) research by an academic institution by one or more students or professors; (2) anticompetitive requests by one or more competitors; (3) requests by disgruntled former employees for nefarious reasons; (4) etc.

In particular embodiments, the system may, for example, maintain a database (e.g., in computer memory) of former employees. In other embodiments, the system may, for example: (1) identify a plurality of IP addresses associated with a particular entity (e.g., academic organization, competitor, etc.); and (2) substantially automatically reject a data subject access request that originates from the plurality of IP addresses. In such embodiments, the system may be configured to automatically add such identified IP addresses and/or domains to the blacklist.

In still other embodiments, the system is configured to maintain a listing of blacklisted names of particular individuals. These may include, for example, one or more individuals identified (e.g., by an organization or other entity) as submitting malicious data subject access requests).

FIG. **47** depicts a queue of pending data subject access requests. As shown in this figure, the first three listed data subject access requests are new and require verification before processing and fulfillment can begin. As shown in this figure, a user (e.g., such as a privacy officer or other privacy controller) may select a particular request, and select an indicia for verifying the request. The user may also optionally select to reject the request. FIG. **48** depicts an authentication window that enables the user to authenticate a particular request. In various embodiments, the user may provide an explanation of why the user is authenticating the request (e.g., because the requestor successfully completed on or more out-of-wallet questions or for any other suitable reason). The user may further submit one or more attachments to support the verification. In this way, the system

may be configured to document that the authentication process was performed for each request (e.g., in case there was an issue with improperly fulfilling a request, the company could show that they are following procedures to prevent such improper processing). In other embodiments, the system may enable the user to provide similar support when rejecting a request (e.g., because the requestor was blacklisted, made excessive requests, etc.).

Data Subject Access Request Fulfillment Cost Determination

In various embodiments, as may be understood in light of this disclosure, fulfilling a data subject access request may be particularly costly. In some embodiments, a company may store data regarding a particular data subject in multiple different locations for a plurality of different reasons as part of a plurality of different processing and other business activities. For example, a particular data subject may be both a customer and an employee of a particular company or organization. Accordingly, in some embodiments, fulfilling a data subject access request for a particular data subject may involve a plurality of different information technology (IT) professionals in a plurality of different departments of a particular company or organization. As such, it may be useful to determine a cost of a particular data subject access request (e.g., particularly because, in some cases, a data subject is entitled to a response to their data subject access request as a matter of right at no charge).

In particular embodiments, in response to receiving a data subject access request, the system may be configured to: (1) assign the request to at least one privacy team member; (2) identify one or more IT teams required to fulfill the request (e.g., one or more IT teams associated with one or more business units that may store personal data related to the request); (3) delegate one or more subtasks of the request to each of the one or more IT teams; (4) receive one or more time logs from each individual involved in the processing and fulfillment of the data subject access request; (5) calculate an effective rate of each individual's time (e.g., based at least in part on the individual's salary, bonus, benefits, chair cost, etc.); (6) calculate an effective cost of fulfilling the data subject access request based at least in part on the one or more time logs and effective rate of each of the individual's time; and (7) apply an adjustment to the calculated effective cost that accounts for one or more external factors (e.g., overhead, etc.) in order to calculate a cost of fulfilling the data subject access request.

In particular embodiments, the system is configured to substantially automatically track an amount of time spent by each individual involved in the processing and fulfillment of the data subject access request. The system may, for example, automatically track an amount of time between each individual opening and closing a ticket assigned to them as part of their role in processing or fulfilling the data subject access request. In other embodiments, the system may determine the time spent based on an amount of time provided by each respective individual (e.g., the individual may track their own time and submit it to the system).

In various embodiments, the system is configured to measure a cost of each particular data subject access request received, and analyze one or more trends in costs of, for example: (1) data subject access requests over time; (2) related data subject access requests; (3) etc. For example, the system may be configured to track and analyze cost and time-to-process trends for one or more social groups, one or more political groups, one or more class action groups, etc. In particular, the system may be configured to identify a particular group from which the system receives particularly costly data subject access request (e.g., former and/or current employees, members of a particular social group, members of a particular political group, etc.).

In particular embodiments, the system may be configured to utilize data subject access request cost data when processing, assigning, and/or fulfilling future data subject access requests (e.g., from a particular identified group, individual, etc.). For example, the system may be configured to prioritize requests that are expected to be less costly and time-consuming (e.g., based on past cost data) over requests identified as being likely more expensive. Alternatively, the system may prioritize more costly and time-consuming requests over less costly ones in the interest of ensuring that the system is able to respond to each request in a reasonable amount of time (e.g., within a time required by law, such as a thirty day period, or any other suitable time period).

Customer Satisfaction Integration with Data Subject Access Requests

In various embodiments, the system may be configured to collect customer satisfaction data, for example: (1) as part of a data subject access request submission form; (2) when providing one or more results of a data subject access request to the data subject; or (3) at any other suitable time. In various embodiments, the customer satisfaction data may be collected in the form of a suitable survey, free-form response questionnaire, or other suitable satisfaction data collection format (e.g., thumbs up vs. thumbs down, etc.).

FIG. **49** depicts an exemplary customer satisfaction survey that may be included as part of a data subject access request form, provided along with the results of a data subject access request, provided in one or more messages confirming receipt of a data subject access request, etc. As shown in the figure, the customer satisfaction survey may relate to how likely a customer (e.g., a data subject) is to recommend the company (e.g., to which the data subject has submitted the request) to a friend (e.g., or colleague). In the example shown in FIG. **49**, the satisfaction survey may relate to a Net Promoter score (NPS), which may indicate a loyalty of a company's customer relationships. Generally speaking, the Net Promoter Score may measure a loyalty that exists between a provider and a consumer. In various embodiments, the provider may include a company, employer, or any other entity. In particular embodiments, the consumer may include a customer, employee, or other respondent to an NPS survey.

In particular embodiments, the question depicted in FIG. **49** is the primary question utilized in calculating a Net Promoter Score (e.g., "how likely is it that you would recommend our company/product/service to a friend or colleague?"). In particular embodiments, the question is presented with responses ranging from 0 (not at all likely) to 10 (extremely likely). In particular embodiments, the question may include any other suitable scale. As may be understood from FIG. **49**, the system may be configured to assign particular categories to particular ratings on the 10 point scale. The system may be configured to track and store responses provided by consumers and calculate an overall NPS score for the provider. The system may be further configured to generate a visual representation of the NPS score, including a total number of responses received for each particular score and category as shown in FIG. **49**.

In various embodiments, the system may be configured to measure data related to any other suitable customer satisfaction method (e.g., in addition to NPS). By integrating a customer satisfaction survey with the data subject access request process, the system may increase a number of consumers that provide one or more responses to the cus-

tomer satisfaction survey. In particular embodiments, the system is configured to require the requestor to respond to the customer satisfaction survey prior to submitting the data subject access request.

Identifying and Deleting Orphaned Data

In particular embodiments, an Orphaned Data Action System is configured to analyze one or more data systems (e.g., data assets), identify one or more pieces of personal data that are one or more pieces of personal data that are not associated with one or more privacy campaigns of the particular organization, and notify one or more individuals of the particular organization of the one or more pieces of personal data that are one or more pieces of personal data that are not associated with one or more privacy campaigns of the particular organization. In various embodiments, one or more processes described herein with respect to the orphaned data action system may be performed by any suitable server, computer, and/or combination of servers and computers.

Various processes performed by the Orphaned Data Action System may be implemented by an Orphaned Data Action Module **5000**. Referring to FIG. **50**, in particular embodiments, the system, when executing the Orphaned Data Action Module **5000**, is configured to: (1) access one or more data assets of a particular organization; (2) scan the one or more data assets to generate a catalog of one or more privacy campaigns and one or more pieces of personal information associated with one or more individuals; (3) store the generated catalog in computer memory; (4) scan one or more data assets based at least in part on the generated catalog to identify a first portion of the one or more pieces of personal data that are one or more pieces of personal data that are not associated with the one or more privacy campaigns; (5) generate an indication that the first portion of one or more pieces of personal data that are not associated with the one or more privacy campaigns of the particular organization is to be removed from the one or more data assets; (6) present the indication to one or more individuals associated with the particular organization; and (7) remove the first portion of the one or more pieces of personal data that are not associated with the one or more privacy campaigns of the particular organization from the one or more data assets.

When executing the Orphaned Data Action Module **5000**, the system begins, at Step **5010**, by accessing one or more data systems associated with the particular entity. The particular entity may include, for example, a particular organization, company, sub-organization, etc. In particular embodiments, the one or more data assets (e.g., data systems) may include, for example, any entity that collects, processes, contains, and/or transfers data (e.g., a software application, "internet of things" computerized device, database, website, data-center, server, etc.). For example, a data asset may include any software or device utilized by a particular entity for data collection, processing, transfer, storage, etc.

In particular embodiments, the system is configured to identify and access the one or more data assets using one or more data modeling techniques. As discussed more fully above, a data model may store the following information: (1) the entity that owns and/or uses a particular data asset; (2) one or more departments within the organization that are responsible for the data asset; (3) one or more software applications that collect data (e.g., personal data) for storage in and/or use by the data asset; (4) one or more particular data subjects (or categories of data subjects) that information is collected from for use by the data asset; (5) one or more particular types of data that are collected by each of the particular applications for storage in and/or use by the data asset; (6) one or more individuals (e.g., particular individuals or types of individuals) that are permitted to access and/or use the data stored in, or used by, the data asset; (7) which particular types of data each of those individuals are allowed to access and use; and (8) one or more data assets (destination assets) that the data is transferred to for other use, and which particular data is transferred to each of those data assets.

As may be understood in light of this disclosure, the system may utilize a data model (e.g., or one or more data models) of data assets associated with a particular entity to identify and access the one or more data assets associated with the particular entity.

Continuing to Step **5020**, the system is configured to scan the one or more data assets to generate a catalog of one or more privacy campaigns and one or more pieces of personal information associated with one or more individuals. The catalog may include a table of the one or more privacy campaigns within the data assets of the particular entity and, for each privacy campaign, the one or more pieces of personal data stored within the data assets of the particular entity that are associated with the particular privacy campaign. In any embodiment described herein, personal data may include, for example: (1) the name of a particular data subject (which may be a particular individual); (2) the data subject's address; (3) the data subject's telephone number; (4) the data subject's e-mail address; (5) the data subject's social security number; (6) information associated with one or more of the data subject's credit accounts (e.g., credit card numbers); (7) banking information for the data subject; (8) location data for the data subject (e.g., their present or past location); (9) internet search history for the data subject; and/or (10) any other suitable personal information, such as other personal information discussed herein.

In some implementations, the system may access, via one or more computer networks, one or more data models that map an association between one or more pieces of personal data stored within one or more data assets of the particular entity and one or more privacy campaigns of the particular entity. As further described herein, the data models may access the data assets of the particular entity and use one or more suitable data mapping techniques to link, or otherwise associate, the one or more pieces of personal data stored within one or more data assets of the particular entity and one or more privacy campaigns of the particular entity. In some implementations, the one or more data models may link, or otherwise associate, a particular individual and each piece of personal data of that particular individual that is stored on one or more data assets of the particular entity.

In some embodiments, the system is configured to generate and populate a data model based at least in part on existing information stored by the system (e.g., in one or more data assets), for example, using one or more suitable scanning techniques. In still other embodiments, the system is configured to access an existing data model that maps personal data stored by one or more organization systems to particular associated processing activities. In some implementations, the system is configured to generate and populate a data model substantially on the fly (e.g., as the system receives new data associated with particular processing activities). For example, a particular processing activity (e.g., privacy campaign) may include transmission of a periodic advertising e-mail for a particular company (e.g., a hardware store). A data model may locate the collected and stored email addresses for customers that elected to receive

(e.g., consented to receipt of) the promotional email within the data assets of the particular entity, and then map each of the stored email addresses to the particular processing activity (i.e., the transmission of a periodic advertising e-mail) within the data assets of the particular entity.

Next, at Step **5030**, the system is configured to store the generated catalog of one or more privacy campaigns and one or more pieces of personal information associated with one or more individuals. In some implementations, the system may receive an indication that a new processing activity (e.g., privacy campaign) has been launched by the particular entity. In response to receiving the indication, the system may modify the one or more data models to map an association between (i) one or more pieces of personal data associated with one or more individuals obtained in connection with the new privacy campaign and (ii) the new privacy campaign initiated by the particular entity. As the system receives one or more pieces of personal data associated with one or more individuals (e.g., an email address signing up to receive information from the particular entity), then the data model associated with the particular processing activity may associate the received personal data with the privacy campaign. In some implementations, one or more data assets may already include the particular personal data (e.g., email address) because the particular individual, for example, previously provided their email address in relation to a different privacy campaign of the particular entity. In response, the system may access the particular personal data and associate that particular personal data with the new privacy campaign.

At Step **5040**, the system is configured to scan one or more data assets based at least in part on the generated catalog to identify a first portion of the one or more pieces of personal data that are one or more pieces of personal data that are not associated with the one or more privacy campaigns. In various embodiments, the system may use the generated catalogue to scan the data assets of the particular entity to identify personal data that has been collected and stored using one or more computer systems operated and/or utilized by a particular organization where the personal data is not currently being used as part of any privacy campaigns, processing activities, etc. undertaken by the particular organization. The one or more pieces of personal data that are not associated with the one or more privacy campaigns may be a portion of the personal data that is stored by the particular entity. In some implementations, the system may analyze the data models to identify the one or more pieces of personal data that are not associated with the one or more privacy campaigns.

When the particular privacy campaign, processing activity, etc. is terminated or otherwise discontinued, the system may determine if any of the associated personal data that has been collected and stored by the particular organization is now orphaned data. In some implementations, in response to the termination of a particular privacy campaign and/or processing activity, (e.g., manually or automatically), the system may be configured to scan one or more data assets based at least in part on the generated catalog or analyze the data models to determine whether any of the personal data that has been collected and stored by the particular organization is now orphaned data (e.g., whether any personal data collected and stored as part of the now-terminated privacy campaign is being utilized by any other processing activity, has some other legal basis for its continued storage, etc.). In some implementations, the system may generate an indication that one or more pieces of personal data that are associated with the terminated one or more privacy campaigns are included in the portion of the one or more pieces of personal data (e.g., orphaned data).

In additional implementations, the system may determine that a particular privacy campaign, processing activity, etc. has not been utilized for a period of time (e.g., a day, a month, a year). In response, the system may be configured to terminate the particular processing activity, processing activity, etc. In some implementations, in response to the system determining that a particular processing activity has not been utilized for a period of time, the system may prompt one or more individuals associated with the particular entity to indicate whether the particular privacy campaign should be terminated or otherwise discontinued.

For example, a particular processing activity may include transmission of a periodic advertising e-mail for a particular company (e.g., a hardware store). As part of the processing activity, the particular company may have collected and stored e-mail addresses for customers that elected to receive (e.g., consented to the receipt of) the promotional e-mails. In response to determining that the particular company has not sent out any promotional e-mails for at least a particular amount of time (e.g., for at least a particular number of months), the system may be configured to: (1) automatically terminate the processing activity; (2) identify any of the personal data collected as part of the processing activity that is now orphaned data (e.g., the e-mail addresses); and (3) automatically delete the identified orphaned data. The processing activity may have ended for any suitable reason (e.g., because the promotion that drove the periodic e-mails has ended). As may be understood in light of this disclosure, because the particular organization no longer has a valid basis for continuing to store the e-mail addresses of the customers once the e-mail addresses are no longer being used to send promotional e-mails, the organization may wish to substantially automate the removal of personal data stored in its computer systems that may place the organization in violation of one or more personal data storage rules or regulations.

Continuing to Step **5050**, the system is configured to generate an indication that the portion of one or more pieces of personal data that are not associated with the one or more privacy campaigns of the particular entity is to be removed from the one or more data assets. At Step **5060**, the system is configured to present the indication to one or more individuals associated with the particular entity. The indication may be an electronic notification to be provided to an individual (e.g., privacy officer) associated with the particular entity. The electronic notification may be, for example, (1) a notification within a software application (e.g., a data management system for the one or more data assets of the particular entity), (2) an email notification, (3) etc.

In some implementations, the indication may enable the individual (e.g., privacy officer of the particular entity) to select a set of the one or more pieces of personal data of the portion of the one or more pieces of personal data to retain based on one or more bases to retain the set of the one or more pieces of personal data.

In particular embodiments, the system may prompt the one or more individuals to provide one or more bases to retain the first set of the one or more pieces of personal data of the first portion of the one or more pieces of personal data that are not associated with the one or more privacy campaigns. In some implementations, in response to receiving the provided one or more valid bases to retain the first set of the one or more pieces of personal data from the one or more individuals associated with the particular entity, submitting the provided one or more valid bases to retain the first set of

the one or more pieces of personal data to one or more second individuals associated with the particular entity for authorization. In response, the system may retain the first set of the one or more pieces of personal data of the first portion of the one or more pieces of personal data from the one or more individuals associated with the particular entity. Further, the system may remove a second set of the one or more pieces of personal data of the first portion of the one or more pieces of personal data that are not associated with the one or more privacy campaigns from the one or more data assets. In particular embodiments, the second set of the one or more pieces of personal data may be different from the first set of the one or more pieces of personal data.

Continuing to Step **5070**, the system is configured to remove, by one or more processors, the first portion of the one or more pieces of personal data that are not associated with the one or more privacy campaigns of the particular entity from the one or more data assets.

Data Testing to Confirm Deletion Under a Right to Erasure

In particular embodiments, a Personal Data Deletion System is configured to: (1) at least partially automatically identify and delete personal data that an entity is required to erase under one or more of the conditions discussed above; and (2) perform one or more data tests after the deletion to confirm that the system has, in fact, deleted any personal data associated with the data subject.

Various processes performed by the Personal Data Deletion System may be implemented by a Personal Data Deletion and Testing Module **5100**. Referring to FIG. **51**, in particular embodiments, the system, when executing the Personal Data Deletion and Testing Module **5100**, is configured to: (1) receive an indication that the entity has completed an erasure of one or more pieces of personal data associated with the data subject under a right of erasure; (2) initiate a test interaction between the data subject and the entity, the test interaction requiring a response from the entity to the data subject; (3) determine whether one or more system associated with the entity have initiated a test interaction response to the data subject based at least in part on the test interaction; (4) in response to determining that the one or more systems associated with the entity have initiated the test interaction response, (a) determine that the entity has not completed the erasure of the one or more pieces of personal data associated with the data subject and (b) automatically take one or more actions with regard to the personal data associated with the data subject.

When executing the Personal Data Deletion and Testing Module **5100**, the system begins, at Step **5110**, by receiving an indication that the entity has completed an erasure of one or more pieces of personal data associated with the data subject under a right of erasure. The particular entity may include, for example, a particular organization, company, sub-organization, etc. In particular embodiments, the one or more computers systems may be configured to store (e.g., in memory) an indication that the data subject's request to delete any of their personal data stored by the one or more computers systems has been processed. Under various legal and industry policies/standards, the organization may have a certain period of time (e.g., a number of days) in order to comply with the one or more requirements related to the deletion or removal of personal data in response to receiving a request from the data subject or in response to identifying one or more of the conditions requiring deletion discussed above. In response to the receiving an indication that the deletion request for the data subject's personal data has been processed or the certain period of time (described above) has passed, the system may be configured to perform a data test to confirm the deletion of the data subject's personal data.

Continuing to Step **5120**, in response to receiving the indication that the entity has completed the erasure, the system is configured to initiate a test interaction between the data subject and the entity, the test interaction requiring a response from the entity to the data subject. In particular embodiments, when performing the data test, the system may be configured to provide an interaction request to the entity on behalf of the data subject. In particular embodiments, the interaction request may include, for example, a request for one or more pieces of data associated with the data subject (e.g., account information, etc.). In various embodiments, the interaction request is a request to contact the data subject (e.g., for any suitable reason). The system may, for example, be configured to substantially automatically complete a contact-request form (e.g., a webform made available by the entity) on behalf of the data subject. In various embodiments, when automatically completing the form on behalf of the data subject, the system may be configured to only provide identifying data, but not to provide any contact data. In response to submitting the interaction request (e.g., submitting the webform), the system may be configured to determine whether the one or more computers systems have generated and/or transmitted a response to the data subject. The system may be configured to determine whether the one or more computers systems have generated and/or transmitted the response to the data subject by, for example, analyzing one or more computer systems associated with the entity to determine whether the one or more computer systems have generated a communication to the data subject (e.g., automatically) for transmission to an e-mail address or other contact method associated with the data subject, generated an action-item for an individual to contact the data subject at a particular contact number, etc.

To perform the data test, for example, the system may be configured to: (1) access (e.g., manually or automatically) a form for the entity (e.g., a web-based "Contact Us" form); (2) input a unique identifier associated with the data subject (e.g., a full name or customer ID number) without providing contact information for the data subject (e.g., mailing address, phone number, email address, etc.); and (3) input a request, within the form, for the entity to contact the data subject to provide information associated with the data subject (e.g., the data subject's account balance with the entity). In response to submitting the form to the entity, the system may be configured to determine whether the data subject is contacted (e.g., via a phone call or email) by the one or more computers systems (e.g., automatically). In some implementations, completing the contact-request form may include providing one or more pieces of identifying data associated with the data subject, the one or more pieces of identifying data comprising data other than contact data. In response to determining that the data subject has been contacted following submission of the form, the system may determine that the one or more computers systems have not fully deleted the data subject's personal data (e.g., because the one or more computers systems must still be storing contact information for the data subject in at least one location).

In particular embodiments, the system is configured to generate one or more test profiles for one or more test data subjects. For each of the one or more test data subjects, the system may be configured to generate and store test profile data such as, for example: (1) name; (2) address; (3) telephone number; (4) e-mail address; (5) social security

number; (6) information associated with one or more credit accounts (e.g., credit card numbers); (7) banking information; (8) location data; (9) internet search history; (10) non-credit account data; and/or (11) any other suitable test data. The system may then be configured to at least initially consent to processing or collection of personal data for the one or more test data subjects by the entity. The system may then request deletion of data of any personal data associated with a particular test data subject. In response to requesting the deletion of data for the particular test data subject, the system may then take one or more actions using the test profile data associated with the particular test data subjects in order to confirm that the one or more computers systems have, in fact, deleted the test data subject's personal data (e.g., any suitable action described herein). The system may, for example, be configured to: (1) initiate a contact request on behalf of the test data subject; (2) attempt to login to one or more user accounts that the system had created for the particular test data subject; and/or (3) take any other action, the effect of which could indicate a lack of complete deletion of the test data subject's personal data.

Next, at Step **5130**, in response to initiating the test interaction, the system is configured to determine whether one or more system associated with the entity have initiated a test interaction response to the data subject based at least in part on the test interaction. In response to determining that the entity has generated a response to the test interaction, the system may be configured to determine that the entity has not complied with the data subject's request (e.g., deletion of their personal data from the one or more computers systems). For example, if the test interaction requests for the entity to locate and provide any personal data the system has stored related to the data subject, then by the system providing a response that includes one or more pieces of personal data related to the data subject, the system may determine that the one or more computers systems have not complied with the request. As described above, the request may be an erasure of one or more pieces of personal data associated with the data subject under a right of erasure. In some implementations, the test interaction response may be any response that includes any one of the one or more pieces of personal data the system indicated was erased under the right of erasure. In some implementations, the test interaction response may not include response that indicates that the one or more pieces of personal data the system indicated was erased under the right of erasure was not found or accessed by the system.

At Step **5140**, in response to determining that the one or more systems associated with the entity have initiated the test interaction response the system is configured to (a) determine that the one or more computers systems have not completed the erasure of the one or more pieces of personal data associated with the data subject, and (b) automatically take one or more actions with regard to the personal data associated with the data subject. In response to determining that the one or more computers systems have not fully deleted a data subject's (e.g., or test data subject's) personal data, the system may then be configured, in particular embodiments, to: (1) flag the data subject's personal data for follow up by one or more privacy officers to investigate the lack of deletion; (2) perform one or more scans of one or more computing systems associated with the entity to identify any residual personal data that may be associated with the data subject; (3) generate a report indicating the lack of complete deletion; and/or (4) take any other suitable action to flag the data subject, personal data, initial request to be forgotten, etc. for follow up.

In various embodiments, the one or more actions may include: (1) identifying the one or more pieces of personal data associated with the data subject that remain stored in the one or more computer systems of the entity; (2) flagging the one or more pieces of personal data associated with the data subject that remain stored in the one or more computer systems of the entity; and (3) providing the flagged one or more pieces of personal data associated with the data subject that remain stored in the one or more computer systems of the entity to an individual associated with the entity.

In various embodiments, the system may monitor compliance by a particular entity with a data subject's request to delete the data subject's personal data from the one or more computers systems associated with a particular entity. The system may, for example, be configured to test to ensure the data has been deleted by: (1) submitting a unique token of data through a webform to a system (e.g., mark to); (2) in response to passage of an expected data retention time, test the system by calling into the system after the passage of the data retention time to search for the unique token. In response to finding the unique token, the system may be configured to determine that the data has not been properly deleted.

The system may provide a communication to the entity that includes a unique identifier associated with the data subject, is performed without using a personal communication data platform, prompts the entity to provide a response by contacting the data subject via a personal communication data platform. In response to providing the communication to the entity, the system may determine whether the data subject has received a response via the personal communication data platform. The system may, in response to determining that the data subject has received the response via the personal communication data platform, determine that the one or more computers systems have not complied with the data subject's request for deletion of their personal data. In response, the system may generate an indication that the one or more computers systems have not complied with the data subject's request for deletion of their personal data by the entity, and digitally store the indication that the one or more computers systems have not complied with the data subject's request for deletion of their personal data in computer memory.

Automatic Preparation for Remediation

In particular embodiments, a Risk Remediation System is configured to substantially automatically determine whether to take one or more actions in response to one or more identified risk triggers. For example, an identified risk trigger may be that a data asset for an organization is hosted in only one particular location thereby increasing the scope of risk if the location were infiltrated (e.g., via cybercrime). In particular embodiments, the system is configured to substantially automatically perform one or more steps related to the analysis of and response to the one or more potential risk triggers discussed above. For example, the system may substantially automatically determine a relevance of a risk posed by (e.g., a risk level) the one or more potential risk triggers based at least in part on one or more previously-determined responses to similar risk triggers. This may include, for example, one or more previously determined responses for the particular entity that has identified the current risk trigger, one or more similarly situated entities, or any other suitable entity or potential trigger.

Various processes performed by the Risk Remediation System may be implemented by a Data Risk Remediation Module **5200**. Referring to FIG. **52**, in particular embodiments, the system, when executing the Data Risk Remedia-

tion Module **5200**, is configured to access risk remediation data for an entity that identifies one or more actions to remediate a risk in response to identifying one or more data assets of the entity potentially affected by one or more risk triggers, receive an indication of an update to the one or more data assets, identify one or more updated risk triggers for an entity based at least in part on the update to the one or more data assets, determine, by using one or more data models associated with the risk remediation data, one or more updated actions to remediate the one or more updated risk triggers, analyze the one or more updated risk triggers to determine a relevance of the risk posed to the entity by the one or more updated risk triggers, and update the risk remediation data to include the one or more updated actions to remediate the risk in response to identifying the one or more updated risk triggers.

When executing the Data Risk Remediation Module **5200**, the system begins, at Step **5210**, by accessing risk remediation data for an entity that identifies one or more actions to remediate a risk in response to identifying one or more data assets of the entity potentially affected by one or more risk triggers. The particular entity may include, for example, a particular organization, company, sub-organization, etc. The one or more data assets may include personal data for clients or customers. In embodiment described herein, personal data may include, for example: (1) the name of a particular data subject (which may be a particular individual); (2) the data subject's address; (3) the data subject's telephone number; (4) the data subject's e-mail address; (5) the data subject's social security number; (6) information associated with one or more of the data subject's credit accounts (e.g., credit card numbers); (7) banking information for the data subject; (8) location data for the data subject (e.g., their present or past location); (9) internet search history for the data subject; and/or (10) any other suitable personal information, such as other personal information discussed herein.

In some implementations, the system may include risk remediation data associated with one or more data assets. The risk remediation data may be default or pre-configured risk remediation data that identifies one or more actions to remediate a risk in response to identifying one or more data assets of the entity potentially affected by one or more risk triggers. In some implementations, the system may have previously updated and/or continuously update the risk remediation data. The risk remediation data may be updated and/or based on aggregate risk remediation data for a plurality of identified risk triggers from one or more organizations, which may include the entity.

The system may analyze the aggregate risk remediation data to determine a remediation outcome for each of the plurality of identified risk triggers and an associated entity response to the particular identified risk trigger of the plurality of identified risk triggers. The remediation outcome is an indication of how well the entity response addressed the identified risk trigger. For example, the remediation outcome can be a numerical (e.g., 1 to 10), an indication of the risk trigger after the entity response was performed (e.g., "high," "medium," or "low"). In response to analyzing the aggregate risk remediation data to determine a remediation outcome for each of the plurality of identified risk triggers and an associated entity response to the particular identified risk trigger of the plurality of identified risk triggers, generating the data model of the one or more data models.

One or more data models for the system may be generated to indicate a recommended entity response based on each identified risk trigger. The one or more risk remediation models base be generated in response to analyzing the aggregate risk remediation data to determine a remediation outcome for each of the plurality of identified risk triggers and an associated entity response to the particular identified risk trigger of the plurality of identified risk triggers. Additionally, the risk remediation data for the entity may include the one or more risk remediation data models with an associated one or more data assets of the entity.

Continuing to Step **5220**, the system is configured to receive an indication of an update to the one or more data assets. In particular embodiments, the system may indicate that a modification has been performed to the one or more data assets. In various embodiments, when a privacy campaign, processing activity, etc. of the particular organization is modified (e.g., add, remove, or update particular information), then the system may the risk remediation data for use in facilitating an automatic assessment of and/or response to future identified risk triggers. The modification may be an addition (e.g., additional data stored to the one or more data assets), a deletion (e.g., removing data stored to the one or more data assets), or a change (e.g., editing particular data or rearranging a configuration of the data associated with the one or more data assets. At Step **5230**, the system is configured to identify one or more updated risk triggers for an entity based at least in part on the update to the one or more data assets. The updated risk triggers may be anything that exposes the one or more data assets of the entity to, for example, a data breach or a loss of data, among others. For example, an identified risk trigger may be that a data asset for an organization is hosted in only one particular location thereby increasing the scope of risk if the location were infiltrated (e.g., via cybercrime).

At Step **5240**, the system is configured to determine, by using one or more data models associated with the risk remediation data, one or more updated actions to remediate the one or more updated risk triggers. As previously described above, the one or more data models for the system may be generated to indicate a recommended entity response based on each identified risk trigger. The one or more risk remediation models base be generated in response to analyzing the aggregate risk remediation data to determine a remediation outcome for each of the plurality of identified risk triggers and an associated entity response to the particular identified risk trigger of the plurality of identified risk triggers.

At Step **5250**, the system is configured to analyze the one or more updated risk triggers to determine a relevance of the risk posed to the entity by the one or more updated risk triggers. In particular embodiments, the system is configured to substantially automatically perform one or more steps related to the analysis of and response to the one or more potential risk triggers discussed above. For example, the system may substantially automatically determine a relevance of a risk posed by (e.g., a risk level) the one or more potential risk triggers based at least in part on one or more previously-determined responses to similar risk triggers. This may include, for example, one or more previously determined responses for the particular entity that has identified the current risk trigger, one or more similarly situated entities, or any other suitable entity or potential trigger. In some embodiments, the system is configured to determine, based at least in part on the one or more data assets and the relevance of the risk, whether to take one or more updated actions in response to the one or more updated risk triggers, and take the one or more updated actions to remediate the risk in response to identifying the one or more updated risk triggers.

Additionally, in some implementations, the system may calculate a risk level based at least in part on the one or more updated risk triggers. The risk level may be compared to a threshold risk level for the entity. The threshold risk level may be pre-determined, or the entity may be able to adjust the threshold risk level (e.g., based on the type of data stored in the particular data asset, a number of data assets involved, etc.). In response to determining that the risk level is greater than or equal to the threshold risk level (i.e., a risk level that is defined as riskier than the threshold risk level or as risky as the threshold risk level), updating the risk remediation data to include the one or more updated actions to remediate the risk in response to identifying the one or more updated risk triggers. The risk level may be, for example, a numerical value (e.g., 1 to 10) or a described value (e.g., "low," "medium," or "high"), among others. In some implementations, calculating the risk level may be based at least in part on the one or more updated risk triggers further comprises comparing the one or more updated risk triggers to (i) one or more previously identified risk triggers, and (ii) one or more previously implemented actions to the one or more previously identified risk triggers.

At Step **5260**, the system continues by updating the risk remediation data to include the one or more updated actions to remediate the risk in response to identifying the one or more updated risk triggers. In various embodiments, the system may automatically (e.g., substantially automatically) update the risk remediation data.

In various embodiments, the system may identify one or more risk triggers for an entity based at least in part on the update to the first data asset of the entity, and in turn, identify a second data asset of the entity potentially affected by the one or more risk triggers based at least in part on an association of a first data asset and the second data asset. The system may then determine, by using one or more data models, one or more first updated actions to remediate the one or more updated risk triggers for the first data asset, and determine, by using one or more data models, one or more second updated actions to remediate the one or more updated risk triggers for the second data asset. In some implementations, the one or more first updated actions to remediate the one or more updated risk triggers for the first data asset may be the same as or different from one or more second updated actions to remediate the one or more updated risk triggers for the second data asset. Further, the system may generate (or update) risk remediation data of the entity to include the one or more first updated actions and the one or more second updated actions to remediate the one or more potential risk triggers.

Central Consent Repository Maintenance and Data Inventory Linking

In particular embodiments, a Central Consent System is configured to provide a third-party data repository system to facilitate the receipt and centralized storage of personal data for each of a plurality of respective data subjects, as described herein. Additionally, the Central Consent System is configured to interface with a centralized consent receipt management system.

Various processes performed by the Central Consent System may be implemented by a Central Consent Module **5300**. Referring to FIG. **53**, in particular embodiments, the system, when executing the Central Consent Module **5300**, is configured to: identify a form used to collect one or more pieces of personal data, determine a data asset of a plurality of data assets of the organization where input data of the form is transmitted, add the data asset to the third-party data repository with an electronic link to the form in response to a user submitting the form, create a unique subject identifier associated with the user, transmit the unique subject identifier (i) to the third-party data repository and (ii) along with the form data provided by the user in the form, to the data asset, and digitally store the unique subject identifier (i) in the third-party data repository and (ii) along with the form data provided by the user in the form, in the data asset.

When executing the Central Consent Module **5300**, the system begins, at Step **5310**, by identifying a form used to collect one or more pieces of personal data. The particular entity may include, for example, a particular organization, company, sub-organization, etc. In particular embodiments, the one or more data assets (e.g., data systems) may include, for example, any processor or database that collects, processes, contains, and/or transfers data (e.g., such as a software application, "internet of things" computerized device, database, website, data-center, server, etc.). The one or more forms may ask for personal data, and the one or more data assets may store personal data for clients or customers. In embodiment described herein, personal data may include, for example: (1) the name of a particular data subject (which may be a particular individual); (2) the data subject's address; (3) the data subject's telephone number; (4) the data subject's e-mail address; (5) the data subject's social security number; (6) information associated with one or more of the data subject's credit accounts (e.g., credit card numbers); (7) banking information for the data subject; (8) location data for the data subject (e.g., their present or past location); (9) internet search history for the data subject; and/or (10) any other suitable personal information, such as other personal information discussed herein.

In particular embodiments, the system is configured to identify a form via one or more method that may include one or more website scanning tools (e.g., web crawling). The system may also receive an indication that a user is completing a form (e.g., a webform via a website) associated with the particular organization (e.g., a form to complete for a particular privacy campaign).

The form may include, for example, one or more fields that include the user's e-mail address, billing address, shipping address, and payment information for the purposes of collected payment data to complete a checkout process on an e-commerce website. The system may, for example, be configured to track data on behalf of an entity that collects and/or processes personal data related to: (1) who consented to the processing or collection of personal data (e.g., the data subject themselves or a person legally entitled to consent on their behalf such as a parent, guardian, etc.); (2) when the consent was given (e.g., a date and time); (3) what information was provided to the consenter at the time of consent (e.g., a privacy policy, what personal data would be collected following the provision of the consent, for what purpose that personal data would be collected, etc.); (4) how consent was received (e.g., one or more copies of a data capture form, webform, etc. via which consent was provided by the consenter); (5) when consent was withdrawn (e.g., a date and time of consent withdrawal if the consenter withdraws consent); and/or (6) any other suitable data related to receipt or withdrawal of consent.

Continuing to Step **5320**, the system is configured to determine one or more data assets of a plurality of data assets of the organization where input data of the form is transmitted. In particular embodiments, the system may determine one or more data assets of the organization that receive the form data provided by the user in the form (e.g., webform). In particular embodiments, the system is configured to identify the one or more data assets using one or

more data modeling techniques. As discussed more fully above, a data model may store the following information: (1) the entity that owns and/or uses a particular data asset (e.g., such as a primary data asset, an example of which is shown in the center of the data model in FIG. **4**); (2) one or more departments within the organization that are responsible for the data asset; (3) one or more software applications that collect data (e.g., personal data) for storage in and/or use by the data asset; (4) one or more particular data subjects (or categories of data subjects) that information is collected from for use by the data asset; (5) one or more particular types of data that are collected by each of the particular applications for storage in and/or use by the data asset; (6) one or more individuals (e.g., particular individuals or types of individuals) that are permitted to access and/or use the data stored in, or used by, the data asset; (7) which particular types of data each of those individuals are allowed to access and use; and (8) one or more data assets (destination assets) that the data is transferred to for other use, and which particular data is transferred to each of those data assets.

As may be understood in light of this disclosure, the system may utilize a data model (e.g., or one or more data models) to identify the one or more data assets associated with the particular entity that receive and/or store particular form data.

At Step **5330**, the system is configured to add the one or more data assets to the third-party data repository with an electronic link to the form. In particular embodiments, a third-party data repository system may electronically link the form to the one or more data assets that processor or store the form data of the form. Next, at Step **5340**, in response to a user submitting the form, the system is configured to create a unique subject identifier associated with the user. The system is configured to generate, for each data subject that completes the form (e.g., a webform), a unique identifier. The system may, for example: (1) receive an indication that the form has been completed with the form including a piece of personal data; (2) identify a data subject associated with the piece of personal data; (3) determine whether the central repository system is currently storing data associated with the data subject; and (4) in response to determining that one or more data assets of the plurality of data assets is not currently storing data associated with the data subject (e.g., because the data subject is a new data subject), generate the unique identifier.

In particular embodiments, the unique identifier may include any unique identifier such as, for example: (1) any of the one or more pieces of personal data collected, stored, and/or processed by the system (e.g., name, first name, last name, full name, address, phone number, e-mail address, etc.); (2) a unique string or hash comprising any suitable number of numerals, letters, or combination thereof; and/or (3) any other identifier that is sufficiently unique to distinguish between a first and second data subject for the purpose of subsequent data retrieval. In particular embodiments, the system is configured to assign a permanent identifier to each particular data subject. In other embodiments, the system is configured to assign one or more temporary unique identifiers to the same data subject.

In particular embodiments, the system is configured to: (1) receive an indication of completion of a form associated with the organization by a data subject; (2) determine, based at least in part on searching a unique subject identifier database (e.g., a third-party data repository), whether a unique subject identifier has been generated for the data subject; (3) in response to determining that a unique subject identifier has been generated for the data subject, accessing the unique subject identifier database; (4) identify the unique subject identifier of the data subject based at least in part on form data provided by the data subject in the completion of the form associated with the organization; and (5) update the unique subject identifier database to include an electronic link between the unique subject identifier of the data subject with each of (i) the form (e.g., including the form data) submitted by the data subject of each respective unique subject identifier, and (ii) one or more data assets that utilize the form data of the form received from the data subject. In this way, as an entity collects additional data for a particular unique data subject (e.g., having a unique subject identifier, hash, etc.), the third party data repository system is configured to maintain a centralized database of data collected, stored, and or processed for each unique data subject (e.g., indexed by unique subject identifier). The system may then, in response to receiving a data subject access request from a particular data subject, fulfill the request substantially automatically (e.g., by providing a copy of the personal data, deleting the personal data, indicating to the entity what personal data needs to be deleted from their system and where it is located, etc.). The system may, for example, automatically fulfill the request by: (1) identifying the unique subject identifier associated with the unique data subject making the request; and (2) retrieving any information associated with the unique data subject based on the unique subject identifier.

Continuing to Step **5350**, the system is configured to transmit the unique subject identifier (i) to the third-party data repository and (ii) along with the form data provided by the user in the form, to the data asset. At Step **5360**, the system is configured to digitally store the unique subject identifier (i) in the third-party data repository and (ii) along with the form data provided by the user in the form, in the data asset. As may understood in light of this disclosure, the system may then be configured to facilitate the receipt and centralized storage of personal data for each of a plurality of respective data subjects and the associated one or more data assets that process or store the form data provided by the data subject.

In particular embodiments, the system may be further configured for receiving a data subject access request from the user, accessing the third-party data repository to identify the unique subject identifier of the user, determining which one or more data assets of the plurality of data assets of the organization include the unique subject identifier, and accessing personal data (e.g., form data) of the user stored in each of the one or more data assets of the plurality of data assets of the organization that include the unique subject identifier. In particular embodiments, the data subject access request may be a subject's rights request where the data subject may be inquiring for the organization to provide all data that the particular organization has obtained on the data subject or a data subject deletion request where the data subject is requesting for the particular organization to delete all data that the particular organization has obtained on the data subject.

In particular embodiments, when the data subject access request is a data subject deletion request, in response to accessing the personal data of the user stored in each of the one or more data assets of the plurality of data assets of the organization that include the unique subject identifier, the system deletes the personal data of the user stored in each of the one or more data assets of the plurality of data assets of the organization that include the unique subject identifier. In some embodiments, when the data subject access request is a data subject deletion request, the system may be config-

ured to: (1) in response to accessing the personal data of the user stored in each of the one or more data assets of the plurality of data assets, automatically determine that a first portion of personal data of the user stored in the one or more data assets has one or more legal bases for continued storage; (2) in response to determining that the first portion of personal data of the user stored in the one or more data assets has one or more legal bases for continued storage, automatically maintain storage of the first portion of personal data of the user stored in the one or more data assets; (3) in response to determining that the first portion of personal data of the user stored in the one or more data assets has one or more legal bases for continued storage, automatically maintaining storage of the first portion of personal data of the user stored in the one or more data assets; and (4) automatically facilitating deletion of a second portion of personal data of the user stored in the one or more data assets for which one or more legal bases for continued storage cannot be determined, wherein the first portion of the personal data of the user stored in the one or more data assets is different from the second portion of personal data of the user stored in the one or more data assets.

Data Transfer Risk Identification and Analysis

In particular embodiments, a Data Transfer Risk Identification System is configured to analyze one or more data systems (e.g., data assets), identify data transfers between/among those systems, apply data transfer rules to each data transfer record, perform a data transfer assessment on each data transfer record based on the data transfer rules to be applied to each data transfer record, and calculate a risk score for the data transfer based at least in part on the one or more data transfer risks associated with the data transfer record.

Various processes performed by the Data Transfer Risk Identification System may be implemented by Data Transfer Risk Identification Module **5400**. Referring to FIG. **54**, in particular embodiments, the system, when executing the Data Transfer Risk Identification Module **5400**, is configured for: (1) creating a data transfer record for a data transfer between a first asset in a first location and a second asset in a second location; (2) accessing a set of data transfer rules that are associated with the data transfer record; (3) performing a data transfer assessment based at least in part on applying the set of data transfer rules on the data transfer record; (4) identifying one or more data transfer risks associated with the data transfer record, based at least in part on the data transfer assessment; (5) calculating a risk score for the data transfer based at least in part on the one or more data transfer risks associated with the data transfer record; and (6) digitally storing the risk score for the data transfer.

When executing the Data Transfer Risk Identification Module **5400**, the system begins, at Step **5410**, by creating a data transfer record for a data transfer between a first asset in a first location and a second asset in a second location. The data transfer record may be created for each transfer of data between a first asset in a first location and a second asset in a second location where the transfer record may also include information regarding the type of data being transferred, a time of the data transfer, an amount of data being transferred, etc. In some embodiments, the system may access a data transfer record that may have already been created by the system.

In various embodiments, the system may be configured to determine in which of the one or more defined plurality of physical locations each particular data system is physically located. In particular embodiments, the system is configured to determine the physical location based at least in part on one or more data attributes of a particular data asset (e.g., data system) using one or more data modeling techniques (e.g., using one or more suitable data modeling techniques described herein). In some embodiments, the system may be configured to determine the physical location of each data asset based at least in part on an existing data model that includes the data asset. In still other embodiments, the system may be configured to determine the physical location based at least in part on an IP address and/or domain of the data asset (e.g., in the case of a computer server or other computing device) or any other identifying feature of a particular data asset.

In particular embodiments, the system is configured to identify one or more data elements stored by the one or more data systems that are subject to transfer (e.g., transfer to the one or more data systems such as from a source asset, transfer from the one or more data systems to a destination asset, etc.). In particular embodiments, the system is configured to identify a particular data element that is subject to such transfer (e.g., such as a particular piece of personal data or other data). In some embodiments, the system may be configured to identify any suitable data element that is subject to transfer and includes personal data.

In any embodiment described herein, personal data may include, for example: (1) the name of a particular data subject (which may be a particular individual); (2) the data subject's address; (3) the data subject's telephone number; (4) the data subject's e-mail address; (5) the data subject's social security number; (6) information associated with one or more of the data subject's credit accounts (e.g., credit card numbers); (7) banking information for the data subject; (8) location data for the data subject (e.g., their present or past location); (9) internet search history for the data subject; and/or (10) any other suitable personal information, such as other personal information discussed herein.

In some embodiments, with regard to the location of the one or more data assets, the system may define a geographic location of the one or more data assets. For example, define each of the plurality of physical locations based at least in part on one or more geographic boundaries. These one or more geographic boundaries may include, for example: (1) one or more countries; (2) one or more continents; (3) one or more jurisdictions (e.g., such as one or more legal jurisdictions); (4) one or more territories; (5) one or more counties; (6) one or more cities; (7) one or more treaty members (e.g., such as members of a trade, defense, or other treaty); and/or (8) any other suitable geographically distinct physical locations.

Continuing to Step **5420**, the system is configured for accessing a set of data transfer rules that are associated with the data transfer record. The system may apply data transfer rules to each data transfer record. The data transfer rules may be configurable to support different privacy frameworks (e.g., a particular data subject type is being transferred from a first asset in the European Union to a second asset outside of the European Union) and organizational frameworks (e.g., to support the different locations and types of data assets within an organization). The applied data transfer rules may be automatically configured by the system (e.g., when an update is applied to privacy rules in a country or region) or manually adjusted by the particular organization (e.g., by a privacy officer of the organization). The data transfer rules to be applied may vary based on the data being transferred.

As may be understood from this disclosure, the transfer of personal data may trigger one or more regulations that govern such transfer. In particular embodiments, personal

data may include any data which relate to a living individual who can be identified: (1) from the data; or (2) from the data in combination with other information which is in the possession of, or is likely to come into the possession of a particular entity. In particular embodiments, a particular entity may collect, store, process, and/or transfer personal data for one or more customers, one or more employees, etc.

In various embodiments, the system is configured to use one or more data models of the one or more data assets (e.g., data systems) to analyze one or more data elements associated with those assets to determine whether the one or more data elements include one or more data elements that include personal data and are subject to transfer. In particular embodiments, the transfer may include, for example: (1) an internal transfer (e.g., a transfer from a first data asset associated with the entity to a second data asset associated with the entity); (2) an external transfer (e.g., a transfer from a data asset associated with the entity to a second data asset associated with a second entity); and/or (3) a collective transfer (e.g., a transfer to a data asset associated with the entity from an external data asset associated with a second entity).

The particular entity may include, for example, a particular organization, company, sub-organization, etc. In particular embodiments, the one or more data assets (e.g., data systems) may include, for example, any entity that collects, processes, contains, and/or transfers data (e.g., such as a software application, "internet of things" computerized device, database, web site, data-center, server, etc.). For example, a first data asset may include any software or device utilized by a particular entity for such data collection, processing, transfer, storage, etc. In various embodiments, the first data asset may be at least partially stored on and/or physically located in a particular location. For example, a server may be located in a particular country, jurisdiction, etc. A piece of software may be stored on one or more servers in a particular location, etc.

In particular embodiments, the system is configured to identify the one or more data systems using one or more data modeling techniques. As discussed more fully above, a data model may store the following information: (1) the entity that owns and/or uses a particular data asset (e.g., such as a primary data asset, an example of which is shown in the center of the data model in FIG. **4**); (2) one or more departments within the organization that are responsible for the data asset; (3) one or more software applications that collect data (e.g., personal data) for storage in and/or use by the data asset; (4) one or more particular data subjects (or categories of data subjects) that information is collected from for use by the data asset; (5) one or more particular types of data that are collected by each of the particular applications for storage in and/or use by the data asset; (6) one or more individuals (e.g., particular individuals or types of individuals) that are permitted to access and/or use the data stored in, or used by, the data asset; (7) which particular types of data each of those individuals are allowed to access and use; and (8) one or more data assets (destination assets) that the data is transferred to for other use, and which particular data is transferred to each of those data assets.

As may be understood in light of this disclosure, the system may utilize a data model (e.g., or one or more data models) of data assets associated with a particular entity to identify the one or more data systems associated with the particular entity.

Next, at Step **5430**, the system is configured for performing a data transfer assessment based at least in part on applying the set of data transfer rules on the data transfer record. The data transfer assessment performed by the system may identify risks associated with the data transfer record. At Step **5440**, the system is configured for identifying one or more data transfer risks associated with the data transfer record, based at least in part on the data transfer assessment. The one or more data transfer risks may include, for example, a source location of the first location of the one or more first data asset of the data transfer, a destination location of the second location of the one or more second data asset of the data transfer, one or more type of data being transferred as part of the data transfer (e.g., personal data or sensitive data), a time of the data transfer (e.g., date, day of the week, time, month, etc.), an amount of data being transferred as part of the data transfer.

Continuing to Step **5450**, the system is configured for calculating a risk score for the data transfer based at least in part on the one or more data transfer risks associated with the data transfer record. The risk score may be calculated in a multitude of ways, and may include one or more data transfer risks such as a source location of the data transfer, a destination location of the data transfer, the type of data being transferred, a time of the data transfer, an amount of data being transferred, etc. Additionally, the system may apply weighting factors (e.g., manually or automatically determined) to the risk factors. Further, in some implementations, the system may include a threshold risk score where a data transfer may be terminated if the data transfer risk score indicates a higher risk than the threshold risk score (e.g., the data transfer risk score being higher than the threshold risk score).

In some embodiments, the system may compare the risk score for the data transfer to a threshold risk score, determine that the risk score for the data transfer is a greater risk than the threshold risk score, and in response to determining that the risk score for the data transfer is a greater risk than the threshold risk score, taking one or more action. The one or more action may include, for example, provide the data transfer record to one or more individuals (e.g., a privacy officer) for review of the data transfer record where the one or more individuals may make a decision to approve the data transfer or terminate the data transfer. In some implementations, the system may automatically terminate the data transfer.

In some implementations, the system may generate a secure link between one or more processors associated with the first asset in the first location and one or more processors associated with the second asset in the second location, and the system may further provide the data transfer via the secure link between the one or more processors associated with the first asset in the first location and the one or more processors associated with the second asset in the second location.

In various embodiments, the system may determine a weighting factor for each of the one or more data transfer risks, determine a risk rating for each of the one or more data transfer risks, and calculate the risk level for the data transfer based upon, for each respective one of the one or more data transfer risks, the risk rating for the respective data transfer risk and the weighting factor for the respective data transfer risk.

At Step **5460**, the system continues by digitally storing the risk score for the data transfer. In various embodiments, the system may continue by transferring the data between the first asset in the first location and the second asset in the second location. In some embodiments, the system may be configured to substantially automatically flag a particular transfer of data as problematic (e.g., because the transfer

does not comply with an applicable regulation). For example, a particular regulation may require data transfers from a first asset to a second asset to be encrypted.

Exemplary System Platform According to Various Embodiments

Various embodiments of any system described herein may be implemented in the context of any suitable system (e.g., a privacy compliance system). For example, any system described herein may be implemented to analyze a particular company or other organization's data assets to generate a data model for one or more processing activities, privacy campaigns, etc. undertaken by the organization. In particular embodiments, the system may implement one or more modules in order to at least partially ensure compliance with one or more regulations (e.g., legal requirements) related to the collection and/or storage of personal data. Various aspects of the system's functionality may be executed by certain system modules, including a Data Model Generation Module **300**, Data Model Population Module **11000**, Data Population Questionnaire Generation Module **1200**, Intelligent Identity Scanning Module **2600**, and Data Subject Access Request Fulfillment Module **2900**. These modules are discussed in greater detail below.

Although these modules are presented as a series of steps, it should be understood in light of this disclosure that various embodiments of the Data Model Generation Module **300**, Data Model Population Module **11000**, Data Population Questionnaire Generation Module **1200**, Intelligent Identity Scanning Module **2600**, and Data Subject Access Request Fulfillment Module **2900** described herein may perform the steps described below in an order other than in which they are presented. In still other embodiments, the Data Model Generation Module **300**, Data Model Population Module **11000**, Data Population Questionnaire Generation Module **1200**, Intelligent Identity Scanning Module **2600**, and Data Subject Access Request Fulfillment Module **2900** may omit certain steps described below. In various other embodiments, the Data Model Generation Module **300**, Data Model Population Module **11000**, Data Population Questionnaire Generation Module **1200**, Intelligent Identity Scanning Module **2600**, and Data Subject Access Request Fulfillment Module **2900** may perform steps in addition to those described (e.g., such as one or more steps described with respect to one or more other modules, etc.).

Data Model Generation Module

In particular embodiments, a Data Model Generation Module **300** is configured to: (1) generate a data model (e.g., a data inventory) for one or more data assets utilized by a particular organization; (2) generate a respective data inventory for each of the one or more data assets; and (3) map one or more relationships between one or more aspects of the data inventory, the one or more data assets, etc. within the data model. In particular embodiments, a data asset (e.g., data system, software application, etc.) may include, for example, any entity that collects, processes, contains, and/or transfers data (e.g., such as a software application, "internet of things" computerized device, database, website, data-center, server, etc.). For example, a first data asset may include any software or device (e.g., server or servers) utilized by a particular entity for such data collection, processing, transfer, storage, etc.

In particular embodiments, a particular data asset, or collection of data assets, may be utilized as part of a particular data processing activity (e.g., direct deposit generation for payroll purposes). In various embodiments, a data model generation system may, on behalf of a particular organization (e.g., entity), generate a data model that encompasses a plurality of processing activities. In other embodiments, the system may be configured to generate a discrete data model for each of a plurality of processing activities undertaken by an organization.

Turning to FIG. **55**, in particular embodiments, when executing the Data Model Generation Module **300**, the system begins, at Step **310**, by generating a data model for one or more data assets and digitally storing the data model in computer memory. The system may, for example, store the data model in the One or More Databases **140** described above (or any other suitable data structure). In various embodiments, generating the data model comprises generating a data structure that comprises information regarding one or more data assets, attributes and other elements that make up the data model. As may be understood in light of this disclosure, the one or more data assets may include any data assets that may be related to one another. In particular embodiments, the one or more data assets may be related by virtue of being associated with a particular entity (e.g., organization). For example, the one or more data assets may include one or more computer servers owned, operated, or utilized by the entity that at least temporarily store data sent, received, or otherwise processed by the particular entity.

In still other embodiments, the one or more data assets may comprise one or more third party assets which may, for example, send, receive and/or process personal data on behalf of the particular entity. These one or more data assets may include, for example, one or more software applications (e.g., such as Expensify to collect expense information, QuickBooks to maintain and store salary information, etc.).

Continuing to step **320**, the system is configured to identify a first data asset of the one or more data assets. In particular embodiments, the first data asset may include, for example, any entity (e.g., system) that collects, processes, contains, and/or transfers data (e.g., such as a software application, "internet of things" computerized device, database, website, data-center, server, etc.). For example, the first data asset may include any software or device utilized by a particular organization for such data collection, processing, transfer, etc. In various embodiments, the first data asset may be associated with a particular processing activity (e.g., the first data asset may make up at least a part of a data flow that relates to the collection, storage, transfer, access, use, etc. of a particular piece of data (e.g., personal data)). Information regarding the first data asset may clarify, for example, one or more relationships between and/or among one or more other data assets within a particular organization. In a particular example, the first data asset may include a software application provided by a third party (e.g., a third party vendor) with which the particular entity interfaces for the purpose of collecting, storing, or otherwise processing personal data (e.g., personal data regarding customers, employees, potential customers, etc.).

In particular embodiments, the first data asset is a storage asset that may, for example: (1) receive one or more pieces of personal data form one or more collection assets; (2) transfer one or more pieces of personal data to one or more transfer assets; and/or (3) provide access to one or more pieces of personal data to one or more authorized individuals (e.g., one or more employees, managers, or other authorized individuals within a particular entity or organization). In a particular embodiment, the first data asset is a primary data asset associated with a particular processing activity around which the system is configured to build a data model associated with the particular processing activity.

In particular embodiments, the system is configured to identify the first data asset by scanning a plurality of

computer systems associated with a particular entity (e.g., owned, operated, utilized, etc. by the particular entity). In various embodiments, the system is configured to identify the first data asset from a plurality of data assets identified in response to completion, by one or more users, of one or more questionnaires.

Advancing to Step **330**, the system generates a first data inventory of the first data asset. The data inventory may comprise, for example, one or more inventory attributes associated with the first data asset such as, for example: (1) one or more processing activities associated with the first data asset; (2) transfer data associated with the first data asset (e.g., how and where the data is being transferred to and/or from); (3) personal data associated with the first data asset (e.g., what type of personal data is collected and/or stored by the first data asset; how, and from where, the data is collected, etc.); (4) storage data associated with the personal data (e.g., whether the data is being stored, protected and deleted); and (5) any other suitable attribute related to the collection, use, and transfer of personal data. In other embodiments, the one or more inventory attributes may comprise one or more other pieces of information such as, for example: (1) the type of data being stored by the first data asset; (2) an amount of data stored by the first data asset; (3) whether the data is encrypted; (4) a location of the stored data (e.g., a physical location of one or more computer servers on which the data is stored); etc. In particular other embodiments, the one or more inventory attributes may comprise one or more pieces of information technology data related to the first data asset (e.g., such as one or more pieces of network and/or infrastructure information, IP address, MAC address, etc.).

In various embodiments, the system may generate the data inventory based at least in part on the type of first data asset. For example, particular types of data assets may have particular default inventory attributes. In such embodiments, the system is configured to generate the data inventory for the first data asset, which may, for example, include one or more placeholder fields to be populated by the system at a later time. In this way, the system may, for example, identify particular inventory attributes for a particular data asset for which information and/or population of data is required as the system builds the data model.

As may be understood in light of this disclosure, the system may, when generating the data inventory for the first data asset, generate one or more placeholder fields that may include, for example: (1) the organization (e.g., entity) that owns and/or uses the first data asset (a primary data asset, which is shown in the center of the data model in FIG. **56**); (2) one or more departments within the organization that are responsible for the first data asset; (3) one or more software applications that collect data (e.g., personal data) for storage in and/or use by the first data asset (e.g., or one or more other suitable collection assets from which the personal data that is collected, processed, stored, etc. by the first data asset is sourced); (4) one or more particular data subjects (or categories of data subjects) that information is collected from for use by the first data asset; (5) one or more particular types of data that are collected by each of the particular applications for storage in and/or use by the first data asset; (6) one or more individuals (e.g., particular individuals or types of individuals) that are permitted to access and/or use the data stored in, or used by, the first data asset; (7) which particular types of data each of those individuals are allowed to access and use; and (8) one or more data assets (destination assets) that the data is transferred to from the first data asset, and which particular data is transferred to each of those data assets.

As may be understood in light of this disclosure, the system may be configured to generate the one or more placeholder fields based at least in part on, for example: (1) the type of the first data asset; (2) one or more third party vendors utilized by the particular organization; (3) a number of collection or storage assets typically associated with the type of the first data asset; and/or (4) any other suitable factor related to the first data asset, its one or more inventory attributes, etc. In other embodiments, the system may substantially automatically generate the one or more placeholders based at least in part on a hierarchy and/or organization of the entity for which the data model is being built. For example, a particular entity may have a marketing division, legal department, human resources department, engineering division, or other suitable combination of departments that make up an overall organization. Other particular entities may have further subdivisions within the organization. When generating the data inventory for the first data asset, the system may identify that the first data asset will have both an associated organization and subdivision within the organization to which it is assigned. In this example, the system may be configured to store an indication in computer memory that the first data asset is associated with an organization and a department within the organization.

Next, at Step **340**, the system modifies the data model to include the first data inventory and electronically links the first data inventory to the first data asset within the data model. In various embodiments, modifying the data model may include configuring the data model to store the data inventory in computer memory, and to digitally associate the data inventory with the first data asset in memory.

FIGS. **4** and **5** show a data model according to a particular embodiment. As shown in these figures, the data model may store the following information for the first data asset: (1) the organization that owns and/or uses the first data asset; (2) one or more departments within the organization that are responsible for the first data asset; (3) one or more applications that collect data (e.g., personal data) for storage in and/or use by the first data asset; (4) one or more particular data subjects that information is collected from for use by the first data asset; (5) one or more collection assets from which the first asset receives data (e.g., personal data); (6) one or more particular types of data that are collected by each of the particular applications (e.g., collection assets) for storage in and/or use by the first data asset; (7) one or more individuals (e.g., particular individuals, types of individuals, or other parties) that are permitted to access and/or use the data stored in or used by the first data asset; (8) which particular types of data each of those individuals are allowed to access and use; and (9) one or more data assets (destination assets) the data is transferred to for other use, and which particular data is transferred to each of those data assets. As shown in FIGS. **6** and **7**, the system may also optionally store information regarding, for example, which business processes and processing activities utilize the first data asset.

As noted above, in particular embodiments, the data model stores this information for each of a plurality of different data assets and may include one or more links between, for example, a portion of the model that provides information for a first particular data asset and a second portion of the model that provides information for a second particular data asset.

Advancing to Step **350**, the system next identifies a second data asset from the one or more data assets. In various embodiments, the second data asset may include one of the one or more inventory attributes associated with the first data asset (e.g., the second data asset may include a collection asset associated with the first data asset, a destination asset or transfer asset associated with the first data asset, etc.). In various embodiments, as may be understood in light of the exemplary data models described below, a second data asset may be a primary data asset for a second processing activity, while the first data asset is the primary data asset for a first processing activity. In such embodiments, the second data asset may be a destination asset for the first data asset as part of the first processing activity. The second data asset may then be associated with one or more second destination assets to which the second data asset transfers data. In this way, particular data assets that make up the data model may define one or more connections that the data model is configured to map and store in memory.

Returning to Step **360**, the system is configured to identify one or more attributes associated with the second data asset, modify the data model to include the one or more attributes, and map the one or more attributes of the second data asset within the data model. The system may, for example, generate a second data inventory for the second data asset that comprises any suitable attribute described with respect to the first data asset above. The system may then modify the data model to include the one or more attributes and store the modified data model in memory. The system may further, in various embodiments, associate the first and second data assets in memory as part of the data model. In such embodiments, the system may be configured to electronically link the first data asset with the second data asset. In various embodiments, such association may indicate a relationship between the first and second data assets in the context of the overall data model (e.g., because the first data asset may serve as a collection asset for the second data asset, etc.).

Next, at Step **370**, the system may be further configured to generate a visual representation of the data model. In particular embodiments, the visual representation of the data model comprises a data map. The visual representation may, for example, include the one or more data assets, one or more connections between the one or more data assets, the one or more inventory attributes, etc.

In particular embodiments, generating the visual representation (e.g., visual data map) of a particular data model (e.g., data inventory) may include, for example, generating a visual representation that includes: (1) a visual indication of a first data asset (e.g., a storage asset), a second data asset (e.g., a collection asset), and a third data asset (e.g., a transfer asset); (2) a visual indication of a flow of data (e.g., personal data) from the second data asset to the first data asset (e.g., from the collection asset to the storage asset); (3) a visual indication of a flow of data (e.g., personal data) from the first data asset to the third data asset (e.g., from the storage asset to the transfer asset); (4) one or more visual indications of a risk level associated with the transfer of personal data; and/or (5) any other suitable information related to the one or more data assets, the transfer of data between/among the one or more data assets, access to data stored or collected by the one or more data assets, etc.

In particular embodiments, the visual indication of a particular asset may comprise a box, symbol, shape, or other suitable visual indicator. In particular embodiments, the visual indication may comprise one or more labels (e.g., a name of each particular data asset, a type of the asset, etc.). In still other embodiments, the visual indication of a flow of data may comprise one or more arrows. In particular embodiments, the visual representation of the data model may comprise a data flow, flowchart, or other suitable visual representation.

In various embodiments, the system is configured to display (e.g., to a user) the generated visual representation of the data model on a suitable display device.

Exemplary Data Models and Visual Representations of Data Models (e.g., Data Maps)

FIGS. **56-62** depict exemplary data models according to various embodiments of the system described herein. FIG. **56**, for example, depicts an exemplary data model that does not include a particular processing activity (e.g., that is not associated with a particular processing activity). As may be understood from the data model shown in this figure, a particular data asset (e.g., a primary data asset) may be associated with a particular company (e.g., organization), or organization within a particular company, sub-organization of a particular organization, etc. In still other embodiments, the particular asset may be associated with one or more collection assets (e.g., one or more data subjects from whom personal data is collected for storage by the particular asset), one or more parties that have access to data stored by the particular asset, one or more transfer assets (e.g., one or more assets to which data stored by the particular asset may be transferred), etc.

As may be understood from FIG. **56**, a particular data model for a particular asset may include a plurality of data elements. When generating the data model for the particular asset, a system may be configured to substantially automatically identify one or more types of data elements for inclusion in the data model, and automatically generate a data model that includes those identified data elements (e.g., even if one or more of those data elements must remain unpopulated because the system may not initially have access to a value for the particular data element). In such cases, the system may be configured to store a placeholder for a particular data element until the system is able to populate the particular data element with accurate data.

As may be further understood from FIG. **56**, the data model shown in FIG. **56** may represent a portion of an overall data model. For example, in the embodiment shown in this figure, the transfer asset depicted may serve as a storage asset for another portion of the data model. In such embodiments, the transfer asset may be associated with a respective one or more of the types of data elements described above. In this way, the system may generate a data model that may build upon itself to comprise a plurality of layers as the system adds one or more new data assets, attributes, etc.

As may be further understood from FIG. **56**, a particular data model may indicate one or more parties that have access to and/or use of the primary asset (e.g., storage asset). In such embodiments, the system may be configured to enable the one or more parties to access one or more pieces of data (e.g., personal data) stored by the storage asset.

As shown in FIG. **56**, the data model may further comprise one or more collection assets (e.g., one or more data assets or individuals from which the storage asset receives data such as personal data). In the exemplary data model (e.g., visual data map) shown in this figure, the collection assets comprise a data subject (e.g., an individual that may provide data to the system for storage in the storage asset) and a collection asset (e.g., which may transfer one or more pieces of data that the collection asset has collected to the storage asset).

FIG. **57** depicts a portion of an exemplary data model that is populated for the primary data asset Gusto. Gusto is a software application that, in the example shown in FIG. **57**, may serve as a human resources service that contains financial, expense, review, time and attendance, background, and salary information for one or more employees of a particular organization (e.g., GeneriTech). In the example of FIG. **57**, the primary asset (e.g., Gusto) may be utilized by the HR (e.g., Human Resources) department of the particular organization (e.g., GeneriTech). Furthermore, the primary asset, Gusto, may collect financial information from one or more data subjects (e.g., employees of the particular organization), receive expense information transferred from Expensify (e.g., expensing software), and receive time and attendance data transferred from Kronos (e.g., timekeeping software). In the example shown in FIG. **57**, access to the information collected and/or stored by Gusto may include, for example: (1) an ability to view and administer salary and background information by HR employees, and (2) an ability to view and administer employee review information by one or more service managers. In the example shown in this figure, personal and other data collected and stored by Gusto (e.g., salary information, etc.) may be transferred to a company banking system, to QuickBooks, and/or to an HR file cabinet.

As may be understood from the example shown in FIG. **57**, the system may be configured to generate a data model based around Gusto that illustrates a flow of personal data utilized by Gusto. The data model in this example illustrates, for example, a source of personal data collected, stored and/or processed by Gusto, a destination of such data, an indication of who has access to such data within Gusto, and an organization and department responsible for the information collected by Gusto. In particular embodiments, the data model and accompanying visual representation (e.g., data map) generated by the system as described in any embodiment herein may be utilized in the context of compliance with one or more record keeping requirements related to the collection, storage, and processing of personal data.

FIGS. **58** and **59** depict an exemplary data model and related example that is similar, in some respects, to the data model and example of FIGS. **56** and **57**. In the example shown in FIGS. **58** and **59**, the exemplary data model and related example include a specific business process and processing activity that is associated with the primary asset (Gusto). In this example, the business process is compensation and the specific processing activity is direct deposit generation in Gusto. As may be understood from this figure, the collection and transfer of data related to the storage asset of Gusto is based on a need to generate direct deposits through Gusto in order to compensate employees. Gusto generates the information needed to conduct a direct deposit (e.g., financial and salary information) and then transmits this information to: (1) a company bank system for execution of the direct deposit; (2) Quickbooks for use in documenting the direct deposit payment; and (3) HR File cabinet for use in documenting the salary info and other financial information.

As may be understood in light of this disclosure, when generating such a data model, particular pieces of data (e.g., data attributes, data elements) may not be readily available to the system. In such embodiment, the system is configured to identify a particular type of data, create a placeholder for such data in memory, and seek out (e.g., scan for and populate) an appropriate piece of data to further populate the data model. For example, in particular embodiments, the system may identify Gusto as a primary asset and recognize that Gusto stores expense information. The system may then be configured to identify a source of the expense information (e.g., Expensify).

FIG. **60** depicts an exemplary screen display **800** that illustrates a visual representation (e.g., visual data map) of a data model (e.g., a data inventory). In the example shown in FIG. **8**, the data map provides a visual indication of a flow of data collected from particular data subjects (e.g., employees **801**). As may be understood from this figure, the data map illustrates that three separate data assets receive data (e.g., which may include personal data) directly from the employees **801**. In this example, these three data assets include Kronos **803** (e.g., a human resources software application), Workday **805** (e.g., a human resources software application), and ADP **807** (e.g., a human resources software application and payment processor). As shown in FIG. **60**, the transfer of data from the employees **801** to these assets is indicated by respective arrows.

As further illustrated in FIG. **60**, the data map indicates a transfer of data from Workday **805** to ADP **807** as well as to a Recovery Datacenter **809** and a London HR File Center **811**. As may be understood in light of this disclosure, the Recovery Datacenter **809** and London HR File Center **811** may comprise additional data assets in the context of the data model illustrated by the data map shown in FIG. **60**. The Recover Datacenter **809** may include, for example, one or more computer servers (e.g., backup servers). The London HR File Center **811** may include, for example, one or more databases (e.g., such as the One or More Databases **140** shown in FIG. **1**). As shown in FIG. **60**, each particular data asset depicted in the data map may be shown along with a visual indication of the type of data asset. For example, Kronos **803**, Workday **805**, and ADP **807** are depicted adjacent a first icon type (e.g., a computer monitor), while Recover Datacenter **809** and London HR File Center **811** are depicted adjacent a second and third icon type respectively (e.g., a server cluster and a file folder). In this way, the system may be configured to visually indicate, via the data model, particular information related to the data model in a relatively minimal manner.

FIG. **61** depicts an exemplary screen display **900** that illustrates a data map of a plurality of assets **905** in tabular form (e.g., table form). As may be understood from this figure, a table that includes one or more inventory attributes of each particular asset **905** in the table may indicate, for example: (1) a managing organization **910** of each respective asset **905**; (2) a hosting location **915** of each respective asset **905** (e.g., a physical storage location of each asset **905**); (3) a type **920** of each respective asset **905**, if known (e.g., a database, software application, server, etc.); (4) a processing activity **925** associated with each respective asset **905**; and/or (5) a status **930** of each particular data asset **905**. In various embodiments, the status **930** of each particular asset **905** may indicate a status of the asset **905** in the discovery process. This may include, for example: (1) a "new" status for a particular asset that has recently been discovered as an asset that processes, stores, or collects personal data on behalf of an organization (e.g., discovered via one or more suitable techniques described herein); (2) an "in discovery" status for a particular asset for which the system is populating or seeking to populate one or more inventory attributes, etc.

FIG. **62** depicts an exemplary data map that includes an asset map of a plurality of data assets **1005**A-F, which may, for example, be utilized by a particular entity in the collection, storage, and/or processing of personal data. As may be

understood in light of this disclosure, the plurality of data assets **1005**A-F may have been discovered using any suitable technique described herein (e.g., one or more intelligent identity scanning techniques, one or more questionnaires, one or more application programming interfaces, etc.). In various embodiments, a data inventory for each of the plurality of data assets **1005**A-F may define, for each of the plurality of data assets **1005**A-F a respective inventory attribute related to a storage location of the data asset.

As may be understood from this figure, the system may be configured to generate a map that indicates a location of the plurality of data assets **1005**A-F for a particular entity. In the embodiment shown in this figure, locations that contain a data asset are indicated by circular indicia that contain the number of assets present at that location. In the embodiment shown in this figure, the locations are broken down by country. In particular embodiments, the asset map may distinguish between internal assets (e.g., first party servers, etc.) and external/third party assets (e.g., third party owned servers or software applications that the entity utilizes for data storage, transfer, etc.).

In some embodiments, the system is configured to indicate, via the visual representation, whether one or more assets have an unknown location (e.g., because the data model described above may be incomplete with regard to the location). In such embodiments, the system may be configured to: (1) identify the asset with the unknown location; (2) use one or more data modeling techniques described herein to determine the location (e.g., such as pinging the asset, generating one or more questionnaires for completion by a suitable individual, etc.); and (3) update a data model associated with the asset to include the location.

Data Model Population Module

In particular embodiments, a Data Model Population Module **11000** is configured to: (1) determine one or more unpopulated inventory attributes in a data model; (2) determine one or more attribute values for the one or more unpopulated inventory attributes; and (3) modify the data model to include the one or more attribute values.

Turning to FIG. **63**, in particular embodiments, when executing the Data Model Population Module **11000**, the system begins, at Step **11100**, by analyzing one or more data inventories for each of the one or more data assets in the data model. The system may, for example, identify one or more particular data elements (e.g., inventory attributes) that make up the one or more data inventories. The system may, in various embodiments, scan one or more data structures associated with the data model to identify the one or more data inventories. In various embodiments, the system is configured to build an inventory of existing (e.g., known) data assets and identify inventory attributes for each of the known data assets.

Continuing to Step **11200**, the system is configured to determine, for each of the one or more data inventories, one or more populated inventory attributes and one or more unpopulated inventory attributes (e.g., and/or one or more unpopulated data assets within the data model). As a particular example related to an unpopulated data asset, when generating and populating a data model, the system may determine that, for a particular asset, there is a destination asset. In various embodiments, the destination asset may be known (e.g., and already stored by the system as part of the data model). In other embodiments, the destination asset may be unknown (e.g., a data element that comprises the destination asset may comprise a placeholder or other indication in memory for the system to populate the unpopulated inventory attribute (e.g., data element).

As another particular example, a particular storage asset may be associated with a plurality of inventory assets (e.g., stored in a data inventory associated with the storage asset). In this example, the plurality of inventory assets may include an unpopulated inventory attribute related to a type of personal data stored in the storage asset. The system may, for example, determine that the type of personal data is an unpopulated inventory asset for the particular storage asset.

Returning to Step **11300**, the system is configured to determine, for each of the one or more unpopulated inventory attributes, one or more attribute values. In particular embodiments, the system may determine the one or more attribute values using any suitable technique (e.g., any suitable technique for populating the data model). In particular embodiments, the one or more techniques for populating the data model may include, for example: (1) obtaining data for the data model by using one or more questionnaires associated with a particular privacy campaign, processing activity, etc.; (2) using one or more intelligent identity scanning techniques discussed herein to identify personal data stored by the system and then map such data to a suitable data model; (3) using one or more application programming interfaces (API) to obtain data for the data model from another software application; and/or (4) using any other suitable technique. Exemplary techniques for determining the one or more attribute values are described more fully below. In other embodiments, the system may be configured to use such techniques or other suitable techniques to populate one or more unpopulated data assets within the data model.

Next, at Step **11400**, the system modifies the data model to include the one or more attribute values for each of the one or more unpopulated inventory attributes. The system may, for example, store the one or more attributes values in computer memory, associate the one or more attribute values with the one or more unpopulated inventory attributes, etc. In still other embodiments, the system may modify the data model to include the one or more data assets identified as filling one or more vacancies left within the data model by the unpopulated one or more data assets.

Continuing to Step **11500**, the system is configured to store the modified data model in memory. In various embodiments, the system is configured to store the modified data model in the One or More Databases **140**, or in any other suitable location. In particular embodiments, the system is configured to store the data model for later use by the system in the processing of one or more data subject access requests. In other embodiments, the system is configured to store the data model for use in one or more privacy impact assessments performed by the system.

Data Model Population Questionnaire Generation Module

In particular embodiments, a Data Population Questionnaire Generation Module **1200** is configured to generate a questionnaire (e.g., one or more questionnaires) comprising one or more questions associated with one or more particular unpopulated data attributes, and populate the unpopulated data attributes based at least in part on one or more responses to the questionnaire. In other embodiments, the system may be configured to populate the unpopulated data attributes based on one or more responses to existing questionnaires.

In various embodiments, the one or more questionnaires may comprise one or more processing activity questionnaires (e.g., privacy impact assessments, data privacy impact assessments, etc.) configured to elicit one or more pieces of data related to one or more undertakings by an organization related to the collection, storage, and/or processing of personal data (e.g., processing activities). In particular embodi-

ments, the system is configured to generate the questionnaire (e.g., a questionnaire template) based at least in part on one or more processing activity attributes, data asset attributes (e.g., inventory attributes), or other suitable attributes discussed herein.

Turning to FIG. **64**, in particular embodiments, when executing the Data Population Questionnaire Generation Module **1200**, the system begins, at Step **1210**, by identifying one or more unpopulated data attributes from a data model. The system may, for example, identify the one or more unpopulated data attributes using any suitable technique described above. In particular embodiments, the one or more unpopulated data attributes may relate to, for example, one or more processing activity or asset attributes such as: (1) one or more processing activities associated with a particular data asset; (2) transfer data associated with the particular data asset (e.g., how and where the data stored and/or collected by the particular data asset is being transferred to and/or from); (3) personal data associated with the particular data assets asset (e.g., what type of personal data is collected and/or stored by the particular data asset; how, and from where, the data is collected, etc.); (4) storage data associated with the personal data (e.g., whether the data is being stored, protected and deleted); and (5) any other suitable attribute related to the collection, use, and transfer of personal data by one or more data assets or via one or more processing activities. In other embodiments, the one or more unpopulated inventory attributes may comprise one or more other pieces of information such as, for example: (1) the type of data being stored by the particular data asset; (2) an amount of data stored by the particular data asset; (3) whether the data is encrypted by the particular data asset; (4) a location of the stored data (e.g., a physical location of one or more computer servers on which the data is stored by the particular data asset); etc.

Continuing to Step **1220**, the system generates a questionnaire (e.g., a questionnaire template) comprising one or more questions associated with one or more particular unpopulated data attributes. As may be understood in light of the above, the one or more particulate unpopulated data attributes may relate to, for example, a particular processing activity or a particular data asset (e.g., a particular data asset utilized as part of a particular processing activity). In various embodiments, the one or more questionnaires comprise one or more questions associated with the unpopulated data attribute. For example, if the data model includes an unpopulated data attribute related to a location of a server on which a particular asset stores personal data, the system may generate a questionnaire associated with a processing activity that utilizes the asset (e.g., or a questionnaire associated with the asset). The system may generate the questionnaire to include one or more questions regarding the location of the server.

Returning to Step **1230**, the system maps one or more responses to the one or more questions to the associated one or more particular unpopulated data attributes. The system may, for example, when generating the questionnaire, associate a particular question with a particular unpopulated data attribute in computer memory. In various embodiments, the questionnaire may comprise a plurality of question/answer pairings, where the answer in the question/answer pairings maps to a particular inventory attribute for a particular data asset or processing activity.

In this way, the system may, upon receiving a response to the particular question, substantially automatically populate the particular unpopulated data attribute. Accordingly, at Step **1240**, the system modifies the data model to populate the one or more responses as one or more data elements for the one or more particular unpopulated data attributes. In particular embodiments, the system is configured to modify the data model such that the one or more responses are stored in association with the particular data element (e.g., unpopulated data attribute) to which the system mapped it at Step **1230**. In various embodiments, the system is configured to store the modified data model in the One or More Databases **140**, or in any other suitable location. In particular embodiments, the system is configured to store the data model for later use by the system in the processing of one or more data subject access requests. In other embodiments, the system is configured to store the data model for use in one or more privacy impact assessments performed by the system.

Continuing to optional Step **1250**, the system may be configured to modify the questionnaire based at least in part on the one or more responses. The system may, for example, substantially dynamically add and/or remove one or more questions to/from the questionnaire based at least in part on the one or more responses (e.g., one or more response received by a user completing the questionnaire). For example, the system may, in response to the user providing a particular inventory attribute or new asset, generates additional questions that relate to that particular inventory attribute or asset. The system may, as the system adds additional questions, substantially automatically map one or more responses to one or more other inventory attributes or assets. For example, in response to the user indicating that personal data for a particular asset is stored in a particular location, the system may substantially automatically generate one or more additional questions related to, for example, an encryption level of the storage, who has access to the storage location, etc.

In still other embodiments, the system may modify the data model to include one or more additional assets, data attributes, inventory attributes, etc. in response to one or more questionnaire responses. For example, the system may modify a data inventory for a particular asset to include a storage encryption data element (which specifies whether the particular asset stores particular data in an encrypted format) in response to receiving such data from a questionnaire. Modification of a questionnaire is discussed more fully below with respect to FIG. **65**.

Data Model Population via Questionnaire Process Flow

FIG. **65** depicts an exemplary process flow **1300** for populating a data model (e.g., modifying a data model to include a newly discovered data asset, populating one or more inventory attributes for a particular processing activity or data asset, etc.). In particular, FIG. **65** depicts one or more exemplary data relationships between one or more particular data attributes (e.g., processing activity attributes and/or asset attributes), a questionnaire template (e.g., a processing activity template and/or a data asset template), a completed questionnaire (e.g., a processing activity assessment and/or a data asset assessment), and a data inventory (e.g., a processing activity inventory and/or an asset inventory). As may be understood from this figure the system is configured to: (1) identify new data assets; (2) generate an asset inventory for identified new data assets; and (3) populate the generated asset inventories. Systems and methods for populating the generated inventories are described more fully below.

As may be understood from FIG. **65**, a system may be configured to map particular processing activity attributes **1320**A to each of: (1) a processing activity template **1330**A; and (2) a processing activity data inventory **1310**A. As may

be understood in light of this disclosure, the processing activity template **1330**A may comprise a plurality of questions (e.g., as part of a questionnaire), which may, for example, be configured to elicit discovery of one or more new data assets. The plurality of questions may each correspond to one or more fields in the processing activity inventory **1310**A, which may, for example, define one or more inventory attributes of the processing activity.

In particular embodiments, the system is configured to provide a processing activity assessment **1340**A to one or more individuals for completion. As may be understood from FIG. **65**, the system is configured to launch the processing activity assessment **1340**A from the processing activity inventory **1310**A and further configured to create the processing activity assessment **1340**A from the processing activity template **1330**A. The processing activity assessment **1340**A may comprise, for example, one or more questions related to the processing activity. The system may, in various embodiments, be configured to map one or more responses provided in the processing activity assessment **1340**A to one or more corresponding fields in the processing activity inventory **1310**A. The system may then be configured to modify the processing activity inventory **1310**A to include the one or more responses, and store the modified inventory in computer memory. In various embodiments, the system may be configured to approve a processing activity assessment **1340**A (e.g., receive approval of the assessment) prior to feeding the processing activity inventory attribute values into one or more fields and/or cells of the inventory.

As may be further understood from FIG. **65**, in response to creating a new asset record (e.g., which the system may create, for example, in response to a new asset discovery via the processing activity assessment **1340**A described immediately above, or in any other suitable manner), the system may generate an asset inventory **1310**B (e.g., a data asset inventory) that defines a plurality of inventory attributes for the new asset (e.g., new data asset).

As may be understood from FIG. **65**, a system may be configured to map particular asset attributes **1320**B to each of: (1) an asset template **1330**B; and (2) an asset inventory **1310**B. As may be understood in light of this disclosure, the asset template **1330**B may comprise a plurality of questions (e.g., as part of a questionnaire), which may, for example, be configured to elicit discovery of one or more processing activities associated with the asset and/or one or more inventory attributes of the asset. The plurality of questions may each correspond to one or more fields in the asset inventory **1310**B, which may, for example, define one or more inventory attributes of the asset.

In particular embodiments, the system is configured to provide an asset assessment **1340**B to one or more individuals for completion. As may be understood from FIG. **65**, the system is configured to launch the asset assessment **1340**B from the asset inventory **1310**B and further configured to create the asset assessment **1340**B from the asset template **1330**B. The asset assessment **1340**B may comprise, for example, one or more questions related to the data asset. The system may, in various embodiments, be configured to map one or more responses provided in the asset assessment **1340**B to one or more corresponding fields in the asset inventory **1310**B. The system may then be configured to modify the asset inventory **1310**B (e.g., and/or a related processing activity inventory **1310**A) to include the one or more responses, and store the modified inventory in computer memory. In various embodiments, the system may be configured to approve an asset assessment **1340**B (e.g., receive approval of the assessment) prior to feeding the asset inventory attribute values into one or more fields and/or cells of the inventory.

FIG. **65** further includes a detail view **1350** of a relationship between particular data attributes **1320**C with an exemplary data inventory **1310**C and a questionnaire template **1330**C. As may be understood from this detail view **1350**, a particular attribute name may map to a particular question title in a template **1330**C as well as to a field name in an exemplary data inventory **1310**C. In this way, the system may be configured to populate (e.g., automatically populate) a field name for a particular inventory **1310**C in response to a user providing a question title as part of a questionnaire template **1330**C. Similarly, a particular attribute description may map to a particular question description in a template **1330**C as well as to a tooltip on a fieldname in an exemplary data inventory **1310**C. In this way, the system may be configured to provide the tooltip for a particular inventory **1310**C that includes the question description provided by a user as part of a questionnaire template **1330**C.

As may be further understood from the detail view **1350** of FIG. **65**, a particular response type may map to a particular question type in a template **1330**C as well as to a field type in an exemplary data inventory **1310**C. A particular question type may include, for example, a multiple choice question (e.g., A, B, C, etc.), a freeform response, an integer value, a drop down selection, etc. A particular field type may include, for example, a memo field type, a numeric field type, an integer field type, a logical field type, or any other suitable field type. A particular data attribute may require a response type of, for example: (1) a name of an organization responsible for a data asset (e.g., a free form response); (2) a number of days that data is stored by the data asset (e.g., an integer value); and/or (3) any other suitable response type.

In still other embodiments, the system may be configured to map a one or more attribute values to one or more answer choices in a template **1330**C as well as to one or more lists and/or responses in a data inventory **1310**C. The system may then be configured to populate a field in the data inventory **1310**C with the one or more answer choices provided in a response to a question template **1330**C with one or more attribute values.

Intelligent Identity Scanning Module

Turning to FIG. **66**, in particular embodiments, the Intelligent Identity Scanning Module **2600** is configured to scan one or more data sources to identify personal data stored on one or more network devices for a particular organization, analyze the identified personal data, and classify the personal data (e.g., in a data model) based at least in part on a confidence score derived using one or more machine learning techniques. The confidence score may be and/or comprise, for example, an indication of the probability that the personal data is actually associated with a particular data subject (e.g., that there is at least an 80% confidence level that a particular phone number is associated with a particular individual.)

When executing the Intelligent Identity Scanning Module **2600**, the system begins, at Step **2610**, by connecting to one or more databases or other data structures, and scanning the one or more databases to generate a catalog of one or more individuals and one or more pieces of personal information associated with the one or more individuals. The system may, for example, be configured to connect to one or more databases associated with a particular organization (e.g., one or more databases that may serve as a storage location for any personal or other data collected, processed, etc. by the

particular organization, for example, as part of a suitable processing activity. As may be understood in light of this disclosure, a particular organization may use a plurality of one or more databases (e.g., the One or More Databases **140** shown in FIG. **1**), a plurality of servers (e.g., the One or More Third Party Servers **160** shown in FIG. **1**), or any other suitable data storage location in order to store personal data and other data collected as part of any suitable privacy campaign, privacy impact assessment, processing activity, etc.

In particular embodiments, the system is configured to scan the one or more databases by searching for particular data fields comprising one or more pieces of information that may include personal data. The system may, for example, be configured to scan and identify one of more pieces of personal data such as: (1) name; (2) address; (3) telephone number; (4) e-mail address; (5) social security number; (6) information associated with one or more credit accounts (e.g., credit card numbers); (7) banking information; (8) location data; (9) internet search history; (10) non-credit account data; and/or (11) any other suitable personal information discussed herein. In particular embodiments, the system is configured to scan for a particular type of personal data (e.g., or one or more particular types of personal data).

The system may, in various embodiments, be further configured to generate a catalog of one or more individuals that also includes one or more pieces of personal information (e.g., personal data) identified for the individuals during the scan. The system may, for example, in response to discovering one or more pieces of personal data in a particular storage location, identify one or more associations between the discovered pieces of personal data. For example, a particular database may store a plurality of individuals' names in association with their respective telephone numbers. One or more other databases may include any other suitable information.

The system may, for example, generate the catalog to include any information associated with the one or more individuals identified in the scan. The system may, for example, maintain the catalog in any suitable format (e.g., a data table, etc.).

Continuing to Step **2620**, the system is configured to scan one or more structured and/or unstructured data repositories based at least in part on the generated catalog to identify one or more attributes of data associated with the one or more individuals. The system may, for example, be configured to utilize information discovered during the initial scan at Step **2610** to identify the one or more attributes of data associated with the one or more individuals.

For example, the catalog generated at Step **2610** may include a name, address, and phone number for a particular individual. The system may be configured, at Step **2620**, to scan the one or more structured and/or unstructured data repositories to identify one or more attributes that are associated with one or more of the particular individual's name, address and/or phone number. For example, a particular data repository may store banking information (e.g., a bank account number and routing number for the bank) in association with the particular individual's address. In various embodiments, the system may be configured to identify the banking information as an attribute of data associated with the particular individual. In this way, the system may be configured to identify particular data attributes (e.g., one or more pieces of personal data) stored for a particular individual by identifying the particular data attributes using information other than the individual's name.

Returning to Step **2630**, the system is configured to analyze and correlate the one or more attributes and metadata for the scanned one or more structured and/or unstructured data repositories. In particular embodiments, the system is configured to correlate the one or more attributes with metadata for the associated data repositories from which the system identified the one or more attributes. In this way, the system may be configured to store data regarding particular data repositories that store particular data attributes.

In particular embodiments, the system may be configured to cross-reference the data repositories that are discovered to store one or more attributes of personal data associated with the one or more individuals with a database of known data assets. In particular embodiments, the system is configured to analyze the data repositories to determine whether each data repository is part of an existing data model of data assets that collect, store, and/or process personal data. In response to determining that a particular data repository is not associated with an existing data model, the system may be configured to identify the data repository as a new data asset (e.g., via asset discovery), and take one or more actions (e.g., such as any suitable actions described herein) to generate and populate a data model of the newly discovered data asset. This may include, for example: (1) generating a data inventory for the new data asset; (2) populating the data inventory with any known attributes associated with the new data asset; (3) identifying one or more unpopulated (e.g., unknown) attributes of the data asset; and (4) taking any suitable action described herein to populate the unpopulated data attributes.

In particular embodiments, the system my, for example: (1) identify a source of the personal data stored in the data repository that led to the new asset discovery; (2) identify one or more relationships between the newly discovered asset and one or more known assets; and/or (3) etc.

Continuing to Step **2640**, the system is configured to use one or more machine learning techniques to categorize one or more data elements from the generated catalog, analyze a flow of the data among the one or more data repositories, and/or classify the one or more data elements based on a confidence score as discussed below.

Continuing to Step **2650**, the system, in various embodiments, is configured to receive input from a user confirming or denying a categorization of the one or more data elements, and, in response, modify the confidence score. In various embodiments, the system is configured to iteratively repeat Steps **2640** and **2650**. In this way, the system is configured to modify the confidence score in response to a user confirming or denying the accuracy of a categorization of the one or more data elements. For example, in particular embodiments, the system is configured to prompt a user (e.g., a system administrator, privacy officer, etc.) to confirm that a particular data element is, in fact, associated with a particular individual from the catalog. The system may, in various embodiments, be configured to prompt a user to confirm that a data element or attribute discovered during one or more of the scans above were properly categorized at Step **2640**.

In particular embodiments, the system is configured to modify the confidence score based at least in part on receiving one or more confirmations that one or more particular data elements or attributes discovered in a particular location during a scan are associated with particular individuals from the catalog. As may be understood in light of this disclosure, the system may be configured to increase the confidence score in response to receiving confirmation that particular types of data elements or attributes discovered

in a particular storage location are typically confirmed as being associated with particular individuals based on one or more attributes for which the system was scanning.

Exemplary Intelligent Identity Scanning Technical Platforms

FIG. **67** depicts an exemplary technical platform via which the system may perform one or more of the steps described above with respect to the Intelligent Identity Scanning Module **2600**. As shown in the embodiment in this figure, an Intelligent Identity Scanning System **2600** comprises an Intelligent Identity Scanning Server **130**, such as the Intelligent Identity Scanning Server **130** described above with respect to FIG. **1**. The Intelligent Identity Scanning Server **130** may, for example, comprise a processing engine (e.g., one or more computer processors). In some embodiments, the Intelligent Identity Scanning Server **130** may include any suitable cloud hosted processing engine (e.g., one or more cloud-based computer servers). In particular embodiments, the Intelligent Identity Scanning Server **130** is hosted in a Microsoft Azure cloud.

In particular embodiments, the Intelligent Identity Scanning Server **130** is configured to sit outside one or more firewalls (e.g., such as the firewall **195** shown in FIG. **26**). In such embodiments, the Intelligent Identity Scanning Server **130** is configured to access One or More Remote Computing Devices **150** through the Firewall **195** (e.g., one or more firewalls) via One or More Networks **115** (e.g., such as any of the One or More Networks **115** described above with respect to FIG. **1**).

In particular embodiments, the One or More Remote Computing Devices **150** include one or more computing devices that make up at least a portion of one or more computer networks associated with a particular organization. In particular embodiments, the one or more computer networks associated with the particular organization comprise one or more suitable servers, one or more suitable databases, one or more privileged networks, and/or any other suitable device and/or network segment that may store and/or provide for the storage of personal data. In the embodiment shown in FIG. **27**, the one or more computer networks associated with the particular organization may comprise One or More Third Party Servers **160**, One or More Databases **140**, etc. In particular embodiments, the One or More Remote Computing Devices **150** are configured to access one or more segments of the one or more computer networks associated with the particular organization. In some embodiments, the one or more computer networks associated with the particular organization comprise One or More Privileged Networks **165**. In still other embodiments, the one or more computer networks comprise one or more network segments connected via one or more suitable routers, one or more suitable network hubs, one or more suitable network switches, etc.

As shown in FIG. **67**, various components that make up one or more parts of the one or more computer networks associated with the particular organization may store personal data (e.g., such as personal data stored on the One or More Third Party Servers **160**, the One or More Databases **140**, etc.). In various embodiments, the system is configured to perform one or more steps related to the Intelligent Identity Scanning Server **2600** in order to identify the personal data for the purpose of generating the catalog of individuals described above (e.g., and/or identify one or more data assets within the organization's network that store personal data)

As further shown in FIG. **67**, in various embodiments, the One or More Remote Computing Devices **150** may store a software application (e.g., the Intelligent Identity Scanning Module). In such embodiments, the system may be configured to provide the software application for installation on the One or More Remote Computing Devices **150**. In particular embodiments, the software application may comprise one or more virtual machines. In particular embodiments, the one or more virtual machines may be configured to perform one or more of the steps described above with respect to the Intelligent Identity Scanning Module **2600** (e.g., perform the one or more steps locally on the One or More Remote Computing Devices **150**).

In various embodiments, the one or more virtual machines may have the following specifications: (1) any suitable number of cores (e.g., 4, 6, 8, etc.); (2) any suitable amount of memory (e.g., 4 GB, 8 GB, 16 GB etc.); (3) any suitable operating system (e.g., CentOS 7.2); and/or (4) any other suitable specification. In particular embodiments, the one or more virtual machines may, for example, be used for one or more suitable purposes related to the Intelligent Identity Scanning System **2700**. These one or more suitable purposes may include, for example, running any of the one or more modules described herein, storing hashed and/or non-hashed information (e.g., personal data, personally identifiable data, catalog of individuals, etc.), storing and running one or more searching and/or scanning engines (e.g., Elasticsearch), etc.

In various embodiments, the Intelligent Identity Scanning System **2700** may be configured to distribute one or more processes that make up part of the Intelligent Identity Scanning Process (e.g., described above with respect to the Intelligent Identity Scanning Module **2600**). The one or more software applications installed on the One or more Remote Computing Devices **150** may, for example, be configured to provide access to the one or more computer networks associated with the particular organization to the Intelligent Identity Scanning Server **130**. The system may then be configured to receive, from the One or more Remote Computing Devices **150** at the Intelligent Identity Scanning Server **130**, via the Firewall **195** and One or More Networks **115**, scanned data for analysis.

In particular embodiments, the Intelligent Identity Scanning System **2700** is configured to reduce an impact on a performance of the One or More Remote Computing Devices **150**, One or More Third Party Servers **160** and other components that make up one or more segments of the one or more computer networks associated with the particular organization. For example, in particular embodiments, the Intelligent Identity Scanning System **2700** may be configured to utilize one or more suitable bandwidth throttling techniques. In other embodiments, the Intelligent Identity Scanning System **2700** is configured to limit scanning (e.g., any of the one or more scanning steps described above with respect to the Intelligent Identity Scanning Module **2600**) and other processing steps (e.g., one or more steps that utilize one or more processing resources) to non-peak times (e.g., during the evening, overnight, on weekends and/or holidays, etc.). In other embodiments, the system is configured to limit performance of such processing steps to backup applications and data storage locations. The system may, for example, use one or more sampling techniques to decrease a number of records required to scan during the personal data discovery process.

FIG. **68** depicts an exemplary asset access methodology that the system may utilize in order to access one or more network devices that may store personal data (e.g., or other personally identifiable information). As may be understood from this figure, the system may be configured to access the one or more network devices using a locally deployed

software application (e.g., such as the software application described immediately above). In various embodiments, the software application is configured to route identity scanning traffic through one or more gateways, configure one or more ports to accept one or more identity scanning connections, etc.

As may be understood from this figure, the system may be configured to utilize one or more credential management techniques to access one or more privileged network portions. The system may, in response to identifying particular assets or personally identifiable information via a scan, be configured to retrieve schema details such as, for example, an asset ID, Schema ID, connection string, credential reference URL, etc. In this way, the system may be configured to identify and store a location of any discovered assets or personal data during a scan.

Data Subject Access Request Fulfillment Module

Turning to FIG. **69**, in particular embodiments, a Data Subject Access Request Fulfillment Module **2900** is configured to receive a data subject access request, process the request, and fulfill the request based at least in part on one or more request parameters. In various embodiments, an organization, corporation, etc. may be required to provide information requested by an individual for whom the organization stores personal data within a certain time period (e.g., 30 days). As a particular example, an organization may be required to provide an individual with a listing of, for example: (1) any personal data that the organization is processing for an individual, (2) an explanation of the categories of data being processed and the purpose of such processing; and/or (3) categories of third parties to whom the data may be disclosed.

Various privacy and security policies (e.g., such as the European Union's General Data Protection Regulation, and other such policies) may provide data subjects (e.g., individuals, organizations, or other entities) with certain rights related to the data subject's personal data that is collected, stored, or otherwise processed by an organization. These rights may include, for example: (1) a right to obtain confirmation of whether a particular organization is processing their personal data; (2) a right to obtain information about the purpose of the processing (e.g., one or more reasons for which the personal data was collected); (3) a right to obtain information about one or more categories of data being processed (e.g., what type of personal data is being collected, stored, etc.); (4) a right to obtain information about one or more categories of recipients with whom their personal data may be shared (e.g., both internally within the organization or externally); (5) a right to obtain information about a time period for which their personal data will be stored (e.g., or one or more criteria used to determine that time period); (6) a right to obtain a copy of any personal data being processed (e.g., a right to receive a copy of their personal data in a commonly used, machine-readable format); (7) a right to request erasure (e.g., the right to be forgotten), rectification (e.g., correction or deletion of inaccurate data), or restriction of processing of their personal data; and (8) any other suitable rights related to the collection, storage, and/or processing of their personal data (e.g., which may be provided by law, policy, industry or organizational practice, etc.).

As may be understood in light of this disclosure, a particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, a particular organization may store personal data in a plurality of different locations which may include one or more known and/or unknown locations. As such, complying with particular privacy and security policies related to personal data (e.g., such as responding to one or more requests by data subjects related to their personal data) may be particularly difficult (e.g., in terms of cost, time, etc.). In particular embodiments, a data subject access request fulfillment system may utilize one or more data model generation and population techniques (e.g., such as any suitable technique described herein) to create a centralized data map with which the system can identify personal data stored, collected, or processed for a particular data subject, a reason for the processing, and any other information related to the processing.

Turning to FIG. **69**, when executing the Data Subject Access Request Fulfillment Module **2900**, the system begins, at Step **2910**, by receiving a data subject access request. In various embodiments, the system receives the request via a suitable web form. In certain embodiments, the request comprises a particular request to perform one or more actions with any personal data stored by a particular organization regarding the requestor. For example, in some embodiments, the request may include a request to view one or more pieces of personal data stored by the system regarding the requestor. In other embodiments, the request may include a request to delete one or more pieces of personal data stored by the system regarding the requestor. In still other embodiments, the request may include a request to update one or more pieces of personal data stored by the system regarding the requestor. In still other embodiments, the request may include a request based on any suitable right afforded to a data subject, such as those discussed above.

Continuing to Step **2920**, the system is configured to process the request by identifying and retrieving one or more pieces of personal data associated with the requestor that are being processed by the system. For example, in various embodiments, the system is configured to identify any personal data stored in any database, server, or other data repository associated with a particular organization. In various embodiments, the system is configured to use one or more data models, such as those described above, to identify this personal data and suitable related information (e.g., where the personal data is stored, who has access to the personal data, etc.). In various embodiments, the system is configured to use intelligent identity scanning (e.g., as described above) to identify the requestor's personal data and related information that is to be used to fulfill the request.

In still other embodiments, the system is configured to use one or more machine learning techniques to identify such personal data. For example, the system may identify particular stored personal data based on, for example, a country in which a website that the data subject request was submitted is based, or any other suitable information.

In particular embodiments, the system is configured to scan and/or search one or more existing data models (e.g., one or more current data models) in response to receiving the request in order to identify the one or more pieces of personal data associated with the requestor. The system may, for example, identify, based on one or more data inventories (e.g., one or more inventory attributes) a plurality of storage locations that store personal data associated with the

requestor. In other embodiments, the system may be configured to generate a data model or perform one or more scanning techniques in response to receiving the request (e.g., in order to automatically fulfill the request).

Returning to Step **2930**, the system is configured to take one or more actions based at least in part on the request. In some embodiments, the system is configured to take one or more actions for which the request was submitted (e.g., display the personal data, delete the personal data, correct the personal data, etc.). In particular embodiments, the system is configured to take the one or more actions substantially automatically. In particular embodiments, in response a data subject submitting a request to delete their personal data from an organization's systems, the system may: (1) automatically determine where the data subject's personal data is stored; and (2) in response to determining the location of the data (which may be on multiple computing systems), automatically facilitate the deletion of the data subject's personal data from the various systems (e.g., by automatically assigning a plurality of tasks to delete data across multiple business systems to effectively delete the data subject's personal data from the systems). In particular embodiments, the step of facilitating the deletion may comprise, for example: (1) overwriting the data in memory; (2) marking the data for overwrite; (2) marking the data as free (e.g., and deleting a directory entry associated with the data); and/or (3) any other suitable technique for deleting the personal data. In particular embodiments, as part of this process, the system uses an appropriate data model (see discussion above) to efficiently determine where all of the data subject's personal data is stored.

Overview of Data Subject Access Requests and Data Subject Verification

Various embodiments of a Data Subject Access Request (DSAR) Processing System are configured to receive a data subject access request, process the request, and fulfill the request based at least in part on one or more request parameters. In various embodiments, an organization, corporation, etc. may be required to provide information requested by an individual for whom the organization stores personal data within a certain time period (e.g., 30 days). As a particular example, an organization may be required to provide an individual with a listing of, for example: (1) any personal data that the organization is processing for an individual, (2) an explanation of the categories of data being processed and the purpose of such processing; and/or (3) categories of third parties to whom the data may be disclosed.

Various privacy and security policies (e.g., such as the European Union's General Data Protection Regulation, and other such policies) may provide data subjects (e.g., individuals, organizations, or other entities) with certain rights related to the data subject's personal data that is collected, stored, or otherwise processed by an organization. These rights may include, for example: (1) a right to obtain confirmation of whether a particular organization is processing their personal data; (2) a right to obtain information about the purpose of the processing (e.g., one or more reasons for which the personal data was collected); (3) a right to obtain information about one or more categories of data being processed (e.g., what type of personal data is being collected, stored, etc.); (4) a right to obtain information about one or more categories of recipients with whom their personal data may be shared (e.g., both internally within the organization or externally); (5) a right to obtain information about a time period for which their personal data will be stored (e.g., or one or more criteria used to determine that time period); (6) a right to obtain a copy of any personal data being processed (e.g., a right to receive a copy of their personal data in a commonly used, machine-readable format); (7) a right to request erasure (e.g., the right to be forgotten), rectification (e.g., correction or deletion of inaccurate data), or restriction of processing of their personal data; and (8) any other suitable rights related to the collection, storage, and/or processing of their personal data (e.g., which may be provided by law, policy, industry or organizational practice, etc.).

As may be understood in light of this disclosure, a particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, a particular organization may store personal data in a plurality of different locations which may include one or more known and/or unknown locations. As such, complying with particular privacy and security policies related to personal data (e.g., such as responding to one or more requests by data subjects related to their personal data) may be particularly difficult (e.g., in terms of cost, time, etc.). In particular embodiments, a data subject access request fulfillment system may utilize one or more data model generation and population techniques (e.g., such as any suitable technique described herein) to create a centralized data map with which the system can identify personal data stored, collected, or processed for a particular data subject, a reason for the processing, and any other information related to the processing.

In various embodiments, the system may be adapted for: (1) automatically verifying an identity of a particular data subject access data subject placing the first data subject access request (DSAR); (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically obtaining, from a particular data model, at least a portion of information requested in the first data subject access request; and (3) after obtaining the at least a portion of the requested information, displaying the obtained information to a user as part of a fulfillment of the first data subject access request. The information requested in the first data subject access request may, for example, comprise at least substantially all (e.g., most or all) of the information regarding the first data subject that is stored within the data model.

In various embodiments, the system is adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor placing the first data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically facilitating an update of personal data that an organization associated with the first webform is processing regarding the particular data subject access requestor.

Similarly, in particular embodiments, the system may be adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor placing the first data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically processing a request, made by the particular data subject access requestor, to opt out of having the organization use

the particular data subject access requestor's personal information in one or more particular ways.

In various embodiments, the system may be configured to verify a residency of an individual submitting a DSAR or other request. The system may, for example, require a resident of a particular state (e.g., California) to provide one or more pieces of evidence to confirm their residency in order to enable the data subject to exercise particular rights related to the submission of DSAR(s). The system may, for example, be configured to prompt a data subject to provide a social security number (e.g., or other piece of identifying information) in order to confirm their identify and verify that a name matched with the identifying information matches an address in the location for which the system is verifying residency.

For example, in particular embodiments, the system may be configured to substantially automatically (e.g., automatically) authenticate and/or verify an identity (e.g., residency) of a data subject using any suitable technique. These techniques may include, for example: (1) one or more credit-based and/or public- or private-information-based verification techniques; (2) one or more company verification techniques (e.g., in the case of a business-to-business data subject access request); (3) one or more techniques involving integration with a company's employee authentication system; (4) one or more techniques involving a company's (e.g., organization's) consumer portal authentication process; (5) etc. Various exemplary techniques for authenticating a data subject are discussed more fully below.

In particular embodiments, when authenticating a data subject (e.g., verifying the data subject's identity), the system may be configured to execute particular identity confirmation steps, for example, by interfacing with one or more external systems (e.g., one or more third-party data aggregation systems). For example, the system, when verifying a data subject's identity, may begin by verifying that a person with the data subject's name, address, social security number, or other identifying characteristic (e.g., which may have been provided by the data subject as part of the data subject access request) actually exists. In various embodiments, the system is configured to interface with (e.g., transmit a search request to) one or more credit reporting agencies (e.g., Experian, Equifax, TransUnion, etc.) to confirm that a person with one or more characteristics provided by the data subject exists. The system may, for example, interface with such credit reporting agencies via a suitable plugin (e.g., software plugin). Additionally, there might be a verification on behalf of a trusted third-party system (e.g., the controller).

In still other embodiments, the system may be configured to utilize one or more other third-party systems (e.g., such as LexisNexis, IDology, RSA, etc.), which may, for example, compile utility and phone bill data, property deeds, rental agreement data, and other public records for various individuals. The system may be configured to interface with one or more such third-party systems to confirm that a person with one or more characteristics provided by the data subject exists.

In still other embodiments, the system may be configured to access one or more public record databases (e.g., property tax records, property ownership and transfer recordings with a state or county authority, etc.). In still other embodiments, the system may be configured to confirm a residency of an individual by: (1) accessing one or more credit records or financial accounts of the individual; and (2) identify a location of at least one financial transaction to determine that the individual resides in the particular jurisdiction/location/etc. (e.g., by confirming a grocery store purchase at a particular location). In still other embodiments, the system may confirm a pattern of financial transactions to confirm a residency of the data subject (e.g., as opposed to relying on a single transaction that may have occurred during a temporary stay in the location).

In still other embodiments, the system may access a driver database (e.g., DMV records) to determine whether the individual holds a driver's license in the jurisdiction, has a car registered in the state/location, etc. The system may further be configured to access one or more educational records for the individual to confirm enrollment (e.g., and therefore residency) in a particular school in the location/state/jurisdiction/etc.

Data Subject Verification Module and Related Methods

As discussed in more detail herein, a data subject may submit a subject access request, for example, to request a listing of any personal information that a particular organization is currently storing regarding the data subject, to request that the personal data be deleted, to opt out of allowing the organization to process the personal data, etc. In various embodiments, an organization, corporation, etc. may be required to provide information requested by an individual for whom the organization stores personal data within a certain time period (e.g., 30 days). As a particular example, an organization may be required to provide an individual with a listing of, for example: (1) any personal data that the organization is processing for an individual, (2) an explanation of the categories of data being processed and the purpose of such processing; and/or (3) categories of third parties to whom the data may be disclosed. Various embodiments of a data subject access request verification system are described more fully below.

In particular embodiments, a Data Subject Verification Module **7000** is configured to receive a data subject access request, verify that the data subject is associated with the particular geographic location, process the request, and fulfill the request based at least in part on one or more request parameters. In various embodiments, an organization, corporation, etc. may be required to provide information requested by an individual for whom the organization stores personal data within a certain time period (e.g., 30 days). As a particular example, an organization may be required to provide an individual with a listing of, for example: (1) any personal data that the organization is processing for an individual, (2) an explanation of the categories of data being processed and the purpose of such processing; and (3) categories of third parties to whom the data may be disclosed. In particular embodiments, when processing a data subject access request, the system may be configured to verify an identity of the data subject prior to processing the request (e.g., or as part of the processing step).

Turning to FIG. **70**, when executing the Data Subject Verification Module **3600**, the system begins, at Step **7010**, by receiving a data subject access request. In various embodiments, the system receives the request via a suitable web form. In certain embodiments, the request comprises a particular request to perform one or more actions with any personal data stored by a particular organization regarding the requestor. For example, in some embodiments, the request may include a request to view one or more pieces of personal data stored by the system regarding the requestor (e.g., a subject's rights request). In other embodiments, the request may include a request to delete one or more pieces of personal data stored by the system regarding the requestor. In still other embodiments, the request may

include a request to update one or more pieces of personal data stored by the system regarding the requestor.

Continuing to Step **7020**, the system is configured for determining that the data subject is associated with a particular geographic location. In some implementations, the data subject, when providing the data subject access request, may identify the particular geographic location. For example, the particular geographic location may be a country, state (or province), county, and/or city of residence of the data subject. The particular geographic location may also be a location where data is transmitted from or transmitted to.

In some implementations, the system may automatically determine a location of the data subject when providing the data subject access request. For example, the system may determine that a data subject is located in a jurisdiction, country, or other geographic location when providing the data subject access request. The system may be configured to determine the data subject's location based at least in part on, for example, a geolocation (e.g., GPS location) of a mobile computing device associated with the data subject, an IP address of one or more computing devices associated with the data subject, etc.). As may be understood in light of this disclosure, one or more different countries, jurisdictions, etc. may impose different rules, regulations, etc. related to data subject access requests, and the collection, storage, and processing of personal data. The system may, for example, require a resident of a particular state (e.g., California) to provide one or more pieces of evidence to confirm their residency in order to enable the data subject to exercise particular rights related to the submission of DSAR(s).

Next, at Step **7030**, the system is configured for verifying that the data subject is associated with the particular geographic location. In various embodiments, verifying that the data subject is associated with the particular geographic location may, for example, limit a risk that a third-party or other entity may gain unlawful or unconsented access to the requestor's personal data. As described above, the particular geographic location associated with the data subject may be a location of residence (e.g., a county, state, county, city, zip code, etc.) of the data subject. In various embodiments, the system may be configured to verify the residence of data subject. One or more different privacy laws or set of privacy laws may pertain to individuals that are residents of particular geographic locations.

In various embodiments, to verify the particular geographic location associated with the data subject, the system may be configured to prompt the data subject to provide one or more additional pieces of information. The additional information called for by the prompt to the data subject may include, for example: (1) at least a portion of the data subject's social security number (e.g., last four digits); (2) an address of the data subject; (3) financial transaction information; and/or (4) any other information which may be useful for verifying the particular geographic location associated with the data subject.

In some embodiments, the system may prompt the user to provide the additional information of one or more images (e.g., using a suitable mobile computing device) of additional information, such as a location or individual identifying document (e.g., utility bill, social security card, driver's license, financial transaction data, address, property tax information, etc.). The data identifying the additional information may be provided by the data subject to the system via a secure terminal or secure link to prevent interception of the data or unwarranted access to the additional information. Additionally, the data identifying the additional information may be encrypted for the transmission of the data.

In particular embodiments, the system may be configured to interface with one or more external systems (e.g., one or more third-party data aggregation systems). For example, the system, when verifying the particular geographic location associated with the data subject, may begin by accessing the one or more third-party data aggregation systems. In various embodiments, the system third-party data aggregation systems may include, for example: (1) one or more credit reporting agencies (e.g., Experian, Equifax, TransUnion, etc.) to determine and confirm information related to a data subject (e.g., location of residence); (2) one or more other third-party systems (e.g., such as LexisNexis, IDology, RSA, etc.), which may, for example, compile utility and phone bill data, property deeds, rental agreement data, and other public records for various individuals; (3) one or more public record databases (e.g., property tax records, property ownership and transfer recordings with a state or county authority, etc.).

In various embodiments, the system may compare the one or more additional pieces of information received from the data subject to corresponding data information accessed via one or more third-party data aggregation systems in order to verify that the data subject is associated with the particular geographic location. For example, the one or more additional pieces of information provided by the data subject may identify an address of the data subject (e.g., a utility bill, driver's license, IP address geo-location of the data subject's computing device that executed the data subject access request at the time of the request), etc.). The system may then access one or more third-party data aggregation systems to determine a property identification address of residence of the data subject based at least in part on accessing the one or more property identification databases (e.g., a property tax record database). Further, the system may compare the address of residence of the data subject identified in the one or more additional pieces of information to the property identification address of residence of the data subject, and in response, the system may verify that the data subject is associated with the particular geographic location based at least in part on the comparing of the address of residence of the data subject identified in the one or more additional pieces of information to the property identification address of residence of the data subject.

In still other embodiments, the system may be configured to confirm a residency of an individual by: (1) accessing one or more credit records or financial accounts of the individual; and (2) identify a location of at least one financial transaction to determine that the individual resides in the particular jurisdiction/location/etc. (e.g., by confirming a grocery store purchase at a particular location). In still other embodiments, the system may confirm a pattern of financial transactions to confirm a residency of the data subject (e.g., as opposed to relying on a single transaction that may have occurred during a temporary stay in the location).

In still other embodiments, the system may access a driver database (e.g., DMV records) to determine whether the individual holds a driver's license in the jurisdiction, has a car registered in the state/location, etc. The system may further be configured to access one or more educational records for the individual to confirm enrollment (e.g., and therefore residency) in a particular school in the location/state/jurisdiction/etc. confirming that the data subject is associated with a particular geographic location based at least in part on the one or more additional pieces of information

In various embodiments, one or more pieces of additional information may not be required to be provided from the

data subject, and the system may access one or more third-party data aggregation systems to verify that the data subject is associated with the particular geographic location. For example, at the time of issuing the data subject access request, the system may identify use geo-location processes to determine a location associated with the data subject's computing device (e.g., identifying an IP address of the computing device) that executed the data subject access request at the time of the request. The location may, for example, correspond to a residence location of the data subject (e.g., the data subject issued the data subject access request from their computing device at their residence). In response, the system may access one or more third-party aggregation system (e.g., property tax record database) to verify that the data subject is associated with the particular geographic location.

At Step **7040**, the system is configured to process the request by identifying, and retrieving one or more pieces of personal data associated with the requestor that are being processed by the system. For example, in various embodiments, the system is configured to identify any personal data stored in any database, server, or other data repository associated with a particular organization. In various embodiments, the system is configured to use one or more data models, such as those described above, to identify this personal data and suitable related information (e.g., where the personal data is stored, who has access to the personal data, etc.). In various embodiments, the system is configured to use intelligent identity scanning (e.g., as described above) to identify the requestor's personal data and related information that is to be used to fulfill the request.

In still other embodiments, the system is configured to use one or more machine learning techniques to identify such personal data. For example, the system may identify particular stored personal data based on, for example, a country in which a web site that the data subject request was submitted is based, or any other suitable information.

Turning to Step **7050**, the system is configured to take one or more actions based at least in part on the request. In some embodiments, the system is configured to take one or more actions for which the request was submitted (e.g., display the personal data, delete the personal data, correct the personal data, etc.). In particular embodiments, the system is configured to take the one or more actions substantially automatically.

Overview of Data Subject Access Requests and Data Subject Cookie Verification

Various embodiments of a Data Subject Access Request (DSAR) Processing System are configured to receive a data subject access request, process the request, and fulfill the request based at least in part on one or more request parameters. In various embodiments, an organization, corporation, etc. may be required to provide information requested by an individual for whom the organization stores personal data within a certain time period (e.g., 30 days). As a particular example, an organization may be required to provide an individual with a listing of, for example: (1) any personal data that the organization is processing for an individual, (2) an explanation of the categories of data being processed and the purpose of such processing; and/or (3) categories of third parties to whom the data may be disclosed.

Various privacy and security policies (e.g., such as the European Union's General Data Protection Regulation, and other such policies) may provide data subjects (e.g., individuals, organizations, or other entities) with certain rights related to the data subject's personal data that is collected, stored, or otherwise processed by an organization. These rights may include, for example: (1) a right to obtain confirmation of whether a particular organization is processing their personal data; (2) a right to obtain information about the purpose of the processing (e.g., one or more reasons for which the personal data was collected); (3) a right to obtain information about one or more categories of data being processed (e.g., what type of personal data is being collected, stored, etc.); (4) a right to obtain information about one or more categories of recipients with whom their personal data may be shared (e.g., both internally within the organization or externally); (5) a right to obtain information about a time period for which their personal data will be stored (e.g., or one or more criteria used to determine that time period); (6) a right to obtain a copy of any personal data being processed (e.g., a right to receive a copy of their personal data in a commonly used, machine-readable format); (7) a right to request erasure (e.g., the right to be forgotten), rectification (e.g., correction or deletion of inaccurate data), or restriction of processing of their personal data; and (8) any other suitable rights related to the collection, storage, and/or processing of their personal data (e.g., which may be provided by law, policy, industry or organizational practice, etc.).

As may be understood in light of this disclosure, a particular organization may undertake a plurality of different privacy campaigns, processing activities, etc. that involve the collection and storage of personal data. In some embodiments, each of the plurality of different processing activities may collect redundant data (e.g., may collect the same personal data for a particular individual more than once), and may store data and/or redundant data in one or more particular locations (e.g., on one or more different servers, in one or more different databases, etc.). In this way, a particular organization may store personal data in a plurality of different locations which may include one or more known and/or unknown locations. As such, complying with particular privacy and security policies related to personal data (e.g., such as responding to one or more requests by data subjects related to their personal data) may be particularly difficult (e.g., in terms of cost, time, etc.). In particular embodiments, a data subject access request fulfillment system may utilize one or more data model generation and population techniques (e.g., such as any suitable technique described herein) to create a centralized data map with which the system can identify personal data stored, collected, or processed for a particular data subject, a reason for the processing, and any other information related to the processing.

In various embodiments, the system may be adapted for: (1) automatically verifying an identity of a particular data subject access data subject placing the data subject access request (DSAR); (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically obtaining, from a particular data model, at least a portion of information requested in the first data subject access request; and (3) after obtaining the at least a portion of the requested information, displaying the obtained information to a user as part of a fulfillment of the first data subject access request. The information requested in the first data subject access request may, for example, comprise at least substantially all (e.g., most or all) of the information regarding the first data subject that is stored within the data model.

In various embodiments, the system is adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor

placing the first data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically facilitating an update of personal data that an organization associated with the first webform is processing regarding the particular data subject access requestor.

Similarly, in particular embodiments, the system may be adapted for: (1) automatically verifying, by at least one computer processor, an identity of a particular data subject access requestor placing the data subject access request; and (2) at least partially in response to verifying the identity of the particular data subject access requestor, automatically processing a request, made by the particular data subject access requestor, to opt out of having the organization use the particular data subject access requestor's personal information in one or more particular ways.

In various embodiments, the system is configured to automatically identify a data subject using a random identifier stored in a cookie. The system may, for example, automatically capture one or more consent records related to the individual data subject based on the cookie data. The system may, for example, use a unique cookie generated in response to a user visiting a website through which the user provided consent for an initial processing of information. The system may then use the cookie data to confirm the identity of the user when the user later submits a DSAR (e.g., to modify consent, request collected data, etc.).

Data Subject Cookie Verification Module and Related Methods

As discussed in more detail herein, a data subject may submit a subject access request, for example, to request a listing of any personal information that a particular organization is currently storing regarding the data subject, to request that the personal data be deleted, to opt out of allowing the organization to process the personal data, etc. In various embodiments, the system is configured to verify an identity of a data subject by using a random identifier stored in a cookie. The system may, for example, automatically capture one or more consent records related to the individual data subject based on the cookie data. The system may, for example, use a unique cookie generated in response to a user visiting a website through which the user provided consent for an initial processing of information. The system may then use the cookie data to confirm the identity of the user when the user later submits a DSAR (e.g., to modify consent, request collected data, etc.).

In particular embodiments, a Data Subject Cookie Verification Module **7100** is configured to receive a request to initiate a transaction between an entity and a data subject, generate (i) a consent receipt for the transaction comprising at least a unique subject identifier and a unique consent receipt key and (ii) a unique cookie to identify the data subject's transaction initiated by the data subject, store the consent receipt for the transaction and the unique cookie, receive a data subject access request from the data subject, verify an identity of the data subject based at least in part on the unique cookie, process the request by identifying one or more pieces of personal data associated with the data subject, and taking one or more actions based at least in part on the data subject access request. In particular embodiments, when processing a data subject access request, the system may be configured to verify an identity of the data subject prior to processing the request (e.g., or as part of the processing step).

Turning to FIG. **71**, when executing the Data Subject Cookie Verification Module **7100**, the system begins, at Step **7110**, by receiving a request to initiate a transaction between an entity and a data subject, the transaction being initiated by the data subject via a user interface and involving collection or processing of personal data associated with the data subject by the entity as part of a processing activity undertaken by the entity that the data subject is consenting to as part of the transaction. In particular embodiments, a third-party consent receipt management system may be configured to manage one or more consent receipts for a particular entity. As may be understood in light of this disclosure, a data subject may access an interaction interface (e.g., via the web) for interacting with a particular entity (e.g., one or more entity systems). The interaction interface (e.g., user interface) may include, for example, a suitable website, web form, user interface etc. The interaction interface may be provided by the entity. Using the interaction interface, a data subject may initiate a transaction with the entity that requires the data subject to provide valid consent (e.g., because the transaction includes the processing of personal data by the entity). The transaction may include, for example: (1) accessing the entity's website; (2) signing up for a user account with the entity; (3) signing up for a mailing list with the entity; (4) a free trial sign up; (5) product registration; and/or (6) any other suitable transaction that may result in collection and/or processing personal data, by the entity, about the data subject.

As may be understood from this disclosure, any particular transaction may record and/or require one or more valid consents from the data subject. For example, the system may require a particular data subject to provide consent for each particular type of personal data that will be collected as part of the transaction. The system may, in various embodiments, be configured to prompt the data subject to provide valid consent, for example, by: (1) displaying, via the interaction interface, one or more pieces of information regarding the consent (e.g., what personal data will be collected, how it will be used, etc.); and (2) prompt the data subject to provide the consent.

In response to the data subject (e.g., or the entity) initiating the transaction, the system may be configured to: (1) generate a unique receipt key (e.g., unique receipt ID); (2) associate the unique receipt key with the data subject (e.g., a unique subject identifier), the entity, and the transaction; and (3) electronically store (e.g., in computer memory) the unique receipt key. The system may further store a unique user ID (e.g., unique subject identifier) associated with the data subject (e.g., a hashed user ID, a unique user ID provided by the data subject, unique ID based on a piece of personal data such as an e-mail address, etc.).

Continuing to Step **7120**, the system is configured for generating: (i) a consent receipt for the transaction comprising at least a unique subject identifier and a unique consent receipt key and (ii) a unique cookie to identify the data subject's transaction initiated by the via the user interface. In various embodiments, a third-party data repository system is configured to facilitate the receipt and centralized storage of personal data for each of a plurality of respective data subjects. In particular embodiments, the system may be configured to: (1) receive personal data associated with a particular data subject (e.g., a copy of the data, a link to a location of where the data is stored, etc.); and (2) store the personal data in a suitable data format (e.g., a data model, a reference table, etc.) for later retrieval. In other embodiments, the system may be configured to receive an indication that personal data has been collected regarding a particular data subject (e.g., collected by a first party system, a software application utilized by a particular entity, etc.).

In particular embodiments, the third party data repository system is configured to: (1) receive an indication that a first party system (e.g., entity) has collected and/or processed a piece of personal data for a data subject; (2) determine a location in which the first party system has stored the piece of personal data; (3) optionally digitally store (e.g., in computer memory) a copy of the piece of personal data and associate, in memory, the piece of personal data with the data subject; and (4) optionally digitally store an indication of the storage location utilized by the first party system for the piece of personal data. In particular embodiments, the system is configured to provide a centralized database, for each particular data subject (e.g., each particular data subject about whom a first party system collects or has collected personally identifiable information), of any personal data processed and/or collected by a particular entity.

In particular embodiments, a third-party data repository system is configured to interface with a consent receipt management system (e.g., such as the consent receipt management system described herein). In particular embodiments, the system may, for example: (1) receive an indication of a consent receipt having an associated unique subject identifier and one or more receipt definitions (e.g., such as any suitable definition described herein); (2) identify, based at least in part on the one or more receipt definitions, one or more pieces of repository data associated with the consent receipt (e.g., one or more data elements or pieces of personal data for which the consent receipt provides consent to process; a storage location of the one or more data elements for which the consent receipt provides consent to process; etc.); (3) digitally store the unique subject identifier in one or more suitable data stores; and (4) digitally associate the unique subject identifier with the one or more pieces of repository data. In particular embodiments, the system is configured to store the personal data provided as part of the consent receipt in association with the unique subject identifier.

As may be understood from this disclosure, any particular transaction may record and/or require one or more valid consents from the data subject. For example, the system may require a particular data subject to provide consent for each particular type of personal data that will be collected as part of the transaction. In response to the data subject (e.g., or the entity) initiating the transaction, the system may be configured to: (1) generate a unique receipt key (e.g., unique receipt ID); (2) associate the unique receipt key with the data subject (e.g., a unique subject identifier), the entity, and the transaction; and (3) electronically store (e.g., in computer memory) the unique receipt key. The system may further store a unique user ID (e.g., unique subject identifier) associated with the data subject (e.g., a hashed user ID, a unique user ID provided by the data subject, unique ID based on a piece of personal data such as an e-mail address, etc.).

In particular embodiments, the unique consent receipt key may be associated with one or more receipt definitions, which may include, for example: (1) the unique transaction ID; (2) an identity of one or more controllers and/or representatives of the entity that is engaging in the transaction with the data subject (e.g., and contact information for the one or more controllers); (3) one or more links to a privacy policy associated with the transaction at the time that consent was given; (4) a listing of one or more data types for which consent to process was provided (e.g., email, MAC address, name, phone number, browsing history, etc.); (5) one or more methods used to collect data for which consent to process was provided (e.g., using one or more cookies, receiving the personal data from the data subject directly, etc.); (6) a description of a service (e.g., a service provided as part of the transaction such as a free trial, user account, etc.); (7) one or more purposes of the processing (e.g., for marketing purposes, to facilitate contact with the data subject, etc.); (8) a jurisdiction (e.g., the European Union, United States, etc.); (9) a legal basis for the collection of personal data (e.g., consent); (10) a type of consent provided by the data subject (e.g. unambiguous, explicit, etc.); (11) one or more categories or identities of other entities to whom the personal data may be transferred; (12) one or more bases of a transfer to a third party entity (e.g., adequacy, binding corporate rules, etc.); (13) a retention period for the personal data (e.g., how long the personal data will be stored); (14) a withdrawal mechanism (e.g., a link to a withdrawal mechanism); (15) a timestamp (e.g., date and time); (16) a unique identifier for the receipt; and/or (17) any other suitable information.

In response to receiving valid consent from the data subject, the system is configured to transmit the unique transaction ID and the unique consent receipt key back to the third-party consent receipt management system for processing and/or storage. In other embodiments, the system is configured to transmit the transaction ID to a data store associated with one or more entity systems (e.g., for a particular entity on behalf of whom the third party consent receipt management system is obtaining and managing validly received consent). In further embodiments, the system is configured to transmit the unique transaction ID, the unique consent receipt key, and any other suitable information related to the validly given consent to the centralized data repository system described above for use in determining whether to store particular data and/or for assigning a unique identifier to a particular data subject for centralized data repository management purposes.

The system may be further configured to transmit a consent receipt to the data subject which may include, for example: (1) the unique transaction ID; (2) the unique consent receipt key; and/or (3) any other suitable data related to the validly provided consent. In some embodiments, the system is configured to transmit a consent receipt in any suitable format (e.g., JSON, HTML, e-mail, text, cookie, etc.). In particular embodiments, the receipt transmitted to the data subject may include a link to a subject rights portal via which the data subject may, for example: (1) view one or more provided valid consents; (2) withdraw consent; (3) etc.

The system is also configured to generate a unique cookie to identify the data subject's transaction initiated by the data subject. The system may, for example, automatically capture one or more consent records related to the individual data subject based on the cookie data. The system may, for example, use a unique cookie generated in response to a user visiting a website through which the user provided consent for an initial processing of information. The system may then use the cookie data to confirm the identity of the user when the user later submits a data subject access request (e.g., to modify consent, request collected data, etc.).

In particular embodiments, when the data subject initiates a transaction, the system may produce a cookie to identify the data subject, and the data subject's initiation of the transaction. The cookie may include, for example, (1) a time stamp associated with the data subject' initiation of the transaction; (2) an identifying characteristic associated with the data subject (e.g., an IP address); (3) a randomly generated set of characters or numbers, etc. In various embodiments, the consent receipt and/or the unique cookie may be

electronically provided to the data subject. Additionally, the unique cookie provided to the data subject may be stored within a web browser associated with an electronic device of the data subject.

Continuing to Step **7130**, the system is configured to store the consent receipt for the transaction and the unique cookie. The consent receipt and the unique cookie may be stored in one or more data assets of the entity, or in a third-party storage location. Additionally, the consent receipt and unique cookie may be stored in a common storage location or in different storage locations. At Step **7140**, the system is configured for receiving a data subject access request. In various embodiments, the system receives the request via a suitable web form. In certain embodiments, the request comprises a particular request to perform one or more actions with any personal data stored by a particular organization regarding the requestor. For example, in some embodiments, the request may include a request to view one or more pieces of personal data stored by the system regarding the requestor (e.g., a subject's rights request). In other embodiments, the request may include a request to delete one or more pieces of personal data stored by the system regarding the requestor. In still other embodiments, the request may include a request to update one or more pieces of personal data stored by the system regarding the requestor (e.g., the data subject).

Continuing to Step **7150**, the system is configured for verifying an identity of the data subject based at least in part on the unique cookie. In various embodiments, the system may compare the unique cookie stored by the system with one more cookie associated with the data subject that is obtained by the data subject (e.g., provided by the data subject (or electronic device of the data subject or accessed by the system)). In particular embodiments, the system may (1) access one or more cookies stored within the web browser associated with the electronic device of the data subject; (2) compare (i) the one or more cookies stored within the web browser associated with the electronic device of the data subject to (ii) the unique cookie. The system may determine that the one or more cookies stored within the web browser associated with the electronic device of the data subject includes the unique cookie, and in response, verify the identity of the data subject. Based on the comparison, the system may determine that the one or more cookies stored within the web browser associated with the electronic device of the data subject does not include the unique cookie. In response, the system may generate a notification to provide to the data subject indicating that the identity of the data subject cannot be verified, which may be electronically transmitted to the data subject. In various embodiments, when the data subject cannot be verified, the system may terminate the data subject access request, and/or one or more other verification or validation methods may be required to initiate the processing of the data subject access request.

At Step **7160**, in response to verifying the identity of the data subject, the system is configured to process the request by identifying, and retrieving one or more pieces of personal data associated with the requestor that are being processed by the system. For example, in various embodiments, the system is configured to identify any personal data stored in any database, server, or other data repository associated with a particular organization. In various embodiments, the system is configured to use one or more data models, such as those described above, to identify this personal data and suitable related information (e.g., where the personal data is stored, who has access to the personal data, etc.). In various embodiments, the system is configured to use intelligent identity scanning (e.g., as described above) to identify the requestor's personal data and related information that is to be used to fulfill the request.

In still other embodiments, the system is configured to use one or more machine learning techniques to identify such personal data. For example, the system may identify particular stored personal data based on, for example, a country in which a web site that the data subject request was submitted is based, or any other suitable information.

Turning to Step **7170**, the system is configured to take one or more actions based at least in part on the request. In some embodiments, the system is configured to take one or more actions for which the request was submitted (e.g., display the personal data, delete the personal data, correct the personal data, etc.). In particular embodiments, the system is configured to take the one or more actions substantially automatically.

Alternative Embodiments

In various embodiments, the system may include a recommendation engine to suggest a response and/or resolution to a privacy-related request based on various factors (country, data subject, subject type, request type, language, etc.). For example, in response to determining that a user is submitting a DSAR request from a certain country, (e.g., based on a lookup of the IP of the user), the system may determine the location of the country, native language of the country, data inventory mapping of business systems based on the type of data subject automatically, etc. The system may further determine (e.g., automatically) a priority for processing the request (based on various regulatory, timeframes for completion and business initiatives determined from metadata related to the request).

In some embodiments, the system may be configured to identify an applicable law or regulation related to the request (e.g., based on an origin location of the request, a citizenship of the requestor, etc.). In some embodiments, the system may assign a workflow for processing the request based on one or more parameters relating to the source of the request. The system may, for example, prioritize requests based on an enforcement level of failures (e.g., failure to properly respond to the request, failure to respond to the request within a specific timeframe, etc.) in various jurisdictions.

In some embodiments, the system may be configured to determine whether the system is required to return actual data to a data subject as part of a DSAR or whether metadata is sufficient. The system may, for example, dynamically determine based on regulations for a particular location whether the system can provide an automated response with metadata (e.g., a type of data stored for the data subject) as opposed to the actual data.

In still other embodiments, the system may be configured for redacting a deletion request (e.g., a DSAR including a request to delete) from a data subject based on the data mapping/inventory and the legal basis for processing a request. The system may, for example, be configured to leverage a data subject request from a data subject and utilize a system to detect the type of request. In response to determining that the request is a request to delete data for a user, the system may be configured to utilize a data map/inventory of processes and information about the legal bases for processing various data elements from the data subject involved in a process and based on the geo-location of the data subject along with a model of the regulatory environment. The system may further be configured to redact or remove parts of the deletion request and only delete data that

is not otherwise required for other legal reasons (e.g. tax, contract obligation, etc.) while still deleting the data tied to consent (e.g., data that requires separate consent for the continued storage of).

In other embodiments, the system is configured to identify and map data to a common data subject profile to aggregate an individual's data in order to automatically generate a subject access request report in response to a request from the individual. The system may, for example: (1) identify a particular processing activity for which the data subject previously provided consent; (2) generate a common data subject profile for the processing activity, where the common data subject profile comprises metadata indicating one or more particular types of data collected by one or more systems as part of the data processing activity; and (3) use one or more data modelling techniques to identify each of the one or more particular types of data for the data subject. For, example, the system may generate a common data subject profile that indicates that the processing activity included the collection or processing of: (1) name; (2) e-mail address; and (3) internet search history. In response to generating the common data subject profile, the system may be configured to identify, for the data subject, each of the particular aspects of the common data subject profile for the particular data subject (e.g., name, e-mail address, and internet search history stored by one or more data systems for a particular entity). In response to identifying each of the pieces of data, the system may be configured to automatically generate a response to the data subject access request (i.e., producing the data for the data subject, deleting, etc.). In various embodiments, the system may be configured to identify a particular category of data from the common data subject profile for which the system is unable to automatically identify. In response, the system may be configured to flag the missing data type for manual review and/or processing. In other embodiments, the system may be configured to initiate a data discovery scan and/or other data discovery process (e.g., in order to locate the missing and/or unidentified data for the particular data subject), for example, using any suitable technique described herein.

In various embodiments, the system is configured to use Data Mapping Data Element classification along with intelligent identity scanning to determine how to treat data in a remote system to fulfill DSAR request. (i.e. upon deletion request, the system may use meta data to invoke different automated actions such as: data deletion, anonymization, or retention).

In various embodiments, the system may be adapted to automatically generate a task for one or more third party systems based on metadata about the data subject of the DSAR. For example, the system may be adapted for: (1) in response to receiving a DSAR, obtaining metadata regarding the data subject; (2) using the metadata to determine one or more automated tasks to assign to one or more third party systems; and (3) automatically orchestrate a completion of the one or more tasks (e.g., by automatically completing the tasks, automatically assigning the tasks for completion, etc.

Examples of metadata that may be used to determine whether to auto-orchestrate a task for a third party system based on a particular DSAR include: (1) the type of request, (2) the location from which the request is being made, (3) current sensitivities to world events, (4) a status of the requestor (e.g., especially loyal customer, important client, competitor, employee, etc.), or (5) any other suitable metadata.

CONCLUSION

Although embodiments above are described in reference to various privacy compliance monitoring systems, it should be understood that various aspects of the system described above may be applicable to other privacy-related systems, or to other types of systems, in general.

While this specification contains many specific embodiment details, these should not be construed as limitations on the scope of any invention or of what may be Concepted, but rather as descriptions of features that may be specific to particular embodiments of particular inventions. Certain features that are described in this specification in the context of separate embodiments may also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment may also be implemented in multiple embodiments separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially Concepted as such, one or more features from a Concepted combination may in some cases be excised from the combination, and the Concepted combination may be directed to a sub-combination or variation of a sub-combination.

Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the embodiments described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems may generally be integrated together in a single software product or packaged into multiple software products.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended Concepts. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for the purposes of limitation.

What is claimed is:

1. A method comprising:

providing, by computing hardware, a query interface that is accessible via a public data network and that is configured for querying a plurality of data storage systems included in a private data network;

receiving, via the query interface and the public data network, a query comprising a data subject access request from a computing device;

accessing, by the computing hardware, a consent receipt key for a transaction associated with processing personal data for a data subject identified by the data subject access request;

accessing, by the computing hardware, transaction data for the transaction;

authenticating, by the computing hardware, the query by comparing the transaction data to the consent receipt key to determine that the transaction data comprises a subset of consent receipt key data associated with the consent receipt key; and

responsive to authenticating the query, facilitating, by the computing hardware, execution of processing operations or network communication for retrieving data

responsive to the data subject access request from the plurality of data storage systems included in the private data network; or

preventing, based on a failure to authenticate the query, execution of the processing operations or performing network communication for retrieving data responsive to the data subject access request from the plurality of data storage systems included in the private data network.

2. The method of claim **1**, wherein accessing the transaction data comprises accessing the transaction data on the computing device.

3. The method of claim **2**, wherein the transaction data comprises a cookie.

4. The method of claim **1**, wherein the transaction data identifies the consent receipt key.

5. The method of claim **1**, wherein:

receiving the query comprises receiving the query via a web browser executing on the computing device; and

accessing the transaction data comprises accessing the transaction data from a cookie store accessible to the web browser.

6. The method of claim **1**, wherein:

the consent receipt key data comprises at least one of a transaction identifier for the transaction, a data subject identifier identifying the data subject, or an indication of consent provided by the data subject for the transaction; and

the transaction data comprises at least one of the transaction identifier, the data subject identifier, and the consent receipt key.

7. A system comprising:

a non-transitory computer-readable medium storing instructions; and

a processing device communicatively coupled to the non-transitory computer-readable medium, wherein, the processing device is configured to execute the instructions and thereby perform operations comprising:

receiving, via a web browser on a user device, a data subject access request associated a data subject, the data subject access request comprising a data subject access request parameter;

accessing a consent receipt key for a transaction involving processing of personal data associated with the data subject as part of a transaction, the consent receipt key indicating consent, by the data subject, for the processing of personal data;

accessing transaction data for the transaction on the user device, the transaction data identifying the consent receipt key;

verifying an identity of the data subject based on receipt definitions associated with the consent receipt key and the transaction data; and

in response to verifying the identity of the data subject, processing the data subject access request based on the data subject access request parameter; or

preventing, based on a failure to verify the identity of the data subject, initiation of processing operations or network communication for retrieving data responsive to the data subject access request from a plurality of storage locations included in a private data network.

8. The system of claim **7**, wherein the transaction data comprises a unique cookie that is accessible to the web browser.

9. The system of claim **8**, wherein the unique cookie and the consent receipt key were generated in response to initiation of the transaction.

10. The system of claim **7**, wherein verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data comprises at least a subset of the receipt definitions.

11. The system of claim **10**, wherein:

the receipt definitions comprise at least one of a transaction identifier for the transaction, a data subject identifier identifying the data subject, or an indication of consent provided by the data subject for the transaction; and

the transaction data comprises at least one of the transaction identifier, the data subject identifier, and the consent receipt key.

12. The system of claim **7**, wherein verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data and the receipt definitions identify the transaction.

13. The system of claim **7**, wherein:

receiving the data subject access request via the web browser on the user device comprises receiving the data subject access request via a public data network; and

processing the data subject access request based on the data subject access request parameter comprises initiating processing operations or network communication for retrieving the personal data from a plurality of storage locations in a private computing network.

14. A non-transitory computer-readable medium storing computer-executable instructions that, when executed by processing hardware, configure the processing hardware to perform operations, comprising:

receiving a data subject access request identifying a data subject, the data subject access request comprising a data subject access request parameter;

accessing a consent receipt key for a transaction involving processing of personal data associated with the data subject as part of a transaction, the consent receipt key indicating consent, by the data subject, for the processing of personal data;

accessing transaction data generated in response to initiation of the transaction;

verifying an identity of the data subject based on receipt definitions associated with the consent receipt key and the transaction data; and

in response to verifying the identity of the data subject, processing the data subject access request based on the data subject access request parameter; or

preventing, based on a failure to verify the identity of the data subject, initiation of processing operations or network communication for retrieving data responsive to the data subject access request from a plurality of storage locations included in a private data network.

15. The non-transitory computer-readable medium of claim **14**, wherein processing the data subject access request based on the data subject access request parameter comprises initiating processing operations or network communication for retrieving the personal data from a plurality of storage locations in a private computing network.

16. The non-transitory computer-readable medium of claim **14**, wherein:

receiving the data subject access request comprises receiving the data subject access request via a web browser executing on a computing device; and

accessing the transaction data comprises accessing the transaction data from a cookie store accessible to the web browser.

17. The non-transitory computer-readable medium of claim **16**, wherein the cookie store is local to the computing device.

18. The non-transitory computer-readable medium of claim **14**, wherein verifying the identity of the data subject based on the receipt definitions and the transaction data comprises confirming that the transaction data comprises at least a subset of the receipt definitions.

* * * * *